HAKEMLİ Denetişim
Ortak Aklın Harmanı
Kamu İç Denetçileri Derneği Meşrutiyet Caddesi Konur Sokak No: 36/6 Kızılay - ANKARA
www.kidder.org.tr/denetisim/ • denetisim@kidder.org.tr
ISSN 1308-8335
Yıl: 13, Sayı: 26, 1-12, 2022

Araştırma Makalesi

ULUSAL MEVZUAT PERSPEKTİFİNDE BİLGİ İŞLEM BİRİMLERİNİN İÇ DENETİMİNDE BİR MODEL ÖNERİSİ

(INTERNAL AUDIT OF IT UNITS IN THE PERSPECTIVE OF NATIONAL LEGISLATION A MODEL SUGGESTION)

Dr. Öğr. Üyesi Yenal ARSLAN[1], Halil İbrahim Özbilger[2]

ÖZ

İç denetçiler, yaptıkları denetimleri belirlenmiş standart ve regülasyonlara dayandırmaktadır. Literatürde, bilişim sistemleri denetiminde kullanılan uluslararası standartlar ve siber güvenlik konusunda birçok çalışma olmasına rağmen ülke regülasyonları hakkında fazlaca çalışma bulunmamaktadır. Yapılan bu çalışmada, Türkiye kamu bilişim yöneticileri ve iç denetçilerine fayda sağlamak ve literatüre katkı sunmak amacıyla kamu kurumlarının uyması gereken mevzuatın derlemesi yapılarak kamu iç denetçileri açısından bir denetim kontrol listesi ortaya konulmuştur.

Anahtar Kelimeler: İç Denetim, Bilgi Teknolojileri, Bilişim Yönetişimi, Uyumluluk

JEL Kodları: M48

ABSTRACT

Internal auditors base their audits on standards and regulations. Although there are many studies on international standards and cyber security used in information systems auditing in the literature, there are not many studies on country regulations. In this study, an audit checklist has been put forward for public internal auditors by compiling the legislation that public institutions must comply with in order to benefit the public information managers and internal auditors of Turkey and contribute to the literature.

Keywords: *Internal Audit, Information Technologies, Information Governance, Compliance.*

JEL Classification: *M48*

1. GİRİŞ

Bilgi ve iletişim teknolojilerindeki gelişmeler; büyük miktarda bilgiyi kullanıma sunmuş, kurumların işlerini yürütme şeklini değiştirmiş, faaliyetlerin daha verimli, etkili, hızlı, anlaşılır bir şekilde yürütülmesini sağlamasının yanında maliyet tasarrufu ve insan hatalarını azaltmıştır. Ancak bu olumlu gelişmeler aynı zamanda kritik operasyonlar ve altyapılar için de önemli riskleri beraberinde getirmiş, veri yönetimi ve kaybı riski, teknolojik operasyonel riskler, veri manipülasyonu riski, bilgi güvenliği riskine de neden olmuştur.

Bilgi güvenliği alanındaki önemli ilerlemelere rağmen yaşanan gelişmeler göstermektedir ki birçok bilgi sistemi hala iç ve/veya dış saldırılara karşı savunmasızdır. Bu durum, yeterli güvenlik önlemlerinin alınmasını, bu saldırıların önlenmesini ve olumsuz sonuçların azaltılmasını gerektirmektedir. Bir kurumun bilgi teknolojisi uygulamalarının,

- Dr. Öğr. Üyesi, Ankara Yıldırım Beyazıt Üniversitesi Mühendislik ve Doğa Bilimleri Fakültesi, Yazılım Mühendisliği Bölümü, Ankara, Orcid Id: 0000-0002-1776-6091, yenalarslan@aybu.edu.tr, Sorumlu Yazar
- İç Denetçi, T.C. Ticaret Bakanlığı İç Denetim Birim Başkanlığı - Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Yönetim Bilimleri Anabilim Dalı Doktora Öğrencisi, Orcid Id: 0000-0002-9137-8855, hiozbilger@hotmail.com

altyapısının, veri kullanımının, politikalarının, prosedürlerinin, yönetiminin, operasyonel süreçlerinin kabul edilmiş standartlara göre incelenmesi ve değerlendirilmesi şeklinde ifade edilen bilgi teknolojisi (BT) denetimi onu yoğun şekilde kullanan çoğu kurum için kritik bir başarı faktörü durumuna gelmiştir.

BT'deki mevcut ve potansiyel riskler dikkate alındığında bilgi güvenliği kontrolü ve süreçlerinin etkinliğini düzenli olarak izlemek ve değerlendirmek gittikçe önemli bir konu haline gelmiştir (NIST, 2013, s. 7). Kurumlar, temel faaliyetler için BT sistemlerine dayanıyorsa, bu sistemlere yönelik risklerin kapsamı ve doğasının farkında da olması gereklidir. Bu nedenle, BT alanında güvenliği sağlamanın ilk adımı, riskleri ve bu risklerle ilgili uygun (örneğin güvenlik riskleri, kullanılabilirlik riskleri, performans riskleri ve uyumluluk riskleri ile ilgili) denetim yöntemlerinin belirlenmesidir.

Öte yandan BT'nin iç denetim faaliyetlerinin etkinliğini artırdığı, iç denetim mesleği üzerinde teknolojik gelişmelerin büyük bir etkiye sahip olduğu kabul edilmesi gereken bir durumdur (Harrison & Datta, 2007). Bu durum; kurumun etkin ve verimli faaliyetlerde bulunmasına yardımcı olması, hem yasal hem de idari düzenlemelere uygunluğunu kanıtlaması, potansiyel zorlukları karşılamaya hazır olup olmadığını teyit etmesi ve belki de en önemlisi, paydaşlara kurumun finansal, operasyonel ve birçok konuda güvence vermesi nedeniyle kurumsal risklere karşı bir tampon görevi gören geleneksel iç denetimin ciddi olarak sorgulanmasını gerektirmiştir (Özbilger, 2021, s. 49).

Araştırmalar, sürekli büyüyen bilgi teknolojilerinin gelişmesi nedeniyle iç denetçilerin geleneksel rolünün değiştiğini de ortaya koymuştur (George, Theofanis & Konstantinos, 2015). Uluslararası İç Denetçiler Örgütü (IIA)'ne göre; önlem alınmazsa ilerleyen dönemlerde en önemli risk faktörü durumuna gelecek BT risklerinin tespiti ve yönetimi hakkında anahtar pozisyonunda olacak iç denetim, risklerin tespiti konusundaki başarısı ve alanda yetişmiş tecrübeli denetçilerin varlığı sayesinde elektronik süreçlerin güvenliği açısından kritik öneme sahip olacaktır (IAA, 2020). Söz konusu analizin en önemli bileşenlerinden biri elbette iç kontrol çerçevesi bağlamında iç denetim fonksiyonunun yeterliliği ve etkinliğidir. BT alanında yaşanan önemli iş dönüşümü kurumların stratejisi ve operasyonlarını fazlasıyla etkilemesi nedeniyle yeni riskleri değerlendirme ve bu risklere maruz kalmayı etkin bir şekilde azaltmak için iç denetim kontrollerini değiştirme ihtiyacını doğurmuş ve iç denetçilerin rolü eskiye nazaran BT bilgisini daha fazla içerecek şekilde genişlemiştir (Stoel, Havelka, & Merhout, 2012, s.68).

Son yıllarda, artan farkındalığa ve çok sayıda ileri teknolojik ve süreç savunma mekanizmasına rağmen BT suçlarının artması sonucu veri bütünlüğü, veri gizliliği ve veri kullanılabilirliği hakkındaki kurumsal siber güvenlik politikaları, risk yönetimi süreçleri ve iç kontrollere uygunluk ve bunların korunmadaki etkinliği ile ilgili bağımsız kanıtlar elde etmek amacıyla gerçekleştirilen (IIA, 2016; FERMA, 2019; IIA, 2020) denetimler kurumun faaliyetlerini geliştirmek için tasarlanan bağımsız, nesnel güvence sağlayan iç denetim uygulamasını hızla gelişen bir alan haline getirmiştir (IIA, 2020). Sağlam iç kontrol ilkeleri, BT ile ilgili risklerin yönetimi ve denetimini üçlü hat modelinde düzenlenmesini önermektedir (COSO, 2019; IIA,2020). Eski haliyle "Üçlü Savunma Hattı" şeklinde isimlendirilen, 2020 yılı içerisinde güncellenerek BT ile ilgili her birinin önemli rollere sahip olduğu "Üçlü Hat Modeli" olarak adlandırılan yeni modele göre; ilk hatta, faaliyetleri yürütürken riske maruz kalan ve bu yönüyle riskleri üstlenerek kabul eden ve yöneten ilgili uygulayıcı birimler yer alırken birinci hattan bağımsız olarak ikinci hatta yer alan kurum çapında riskin daha fazla tanımlanmasından, ölçülmesinden, izlenmesinden ve raporlanmasından sorumlu BT ile ilgili birimler yer almaktadır. İç denetim işlevi ise, üçüncü hattan sorumludur: risk yönetişimi ve iç kontrol çerçevesi dâhil olmak üzere genel BT çerçevesinin etkin olduğuna dair kuruma güvence sağlamak için BT ile ilgili riske dayalı denetimler ve incelemeler gerçekleştirir. Bu nedenle, ilk iki hattın bağımsız bir şekilde gözden geçirilmesinden ve iş alanlarındaki mevcut ana zayıflıkları ele alarak kurum içinde proaktif olarak en iyi uygulamaları teşvik etmekten sorumlu olan iç denetim fonksiyonunun diğer denetim türlerinde olduğu gibi bilgi teknolojileri denetiminde de hayati ve önemli bir role sahip olduğunu söylemeye gerek yoktur (Deloitte, 2017).

Avrupa İç Denetçiler Enstitüsü Konfederasyonu (ECIIA) tarafından yürütülen çalışma sonuçlarına göre, BT alanındaki riskler gelecek ilk beş iş riskinden biri olarak kabul edilmiştir (ECIIA, 2020). Ancak, BT denetiminin pratikte nasıl yürütüldüğüne dair tanımlamalar hala büyük ölçüde eksiktir. Bu nedenle özellikle Türkiye gibi iç denetimin olgunlaşamadığı ülkelerde özellikle BT denetiminin etkinliğini ölçmek oldukça zordur. İç denetim fonksiyonunun amacı, kabul edilebilir bir risk düzeyine ulaşmak ve kayıpları en aza indirmek olmasına rağmen bu alandaki faaliyetler genellikle ya BT konusundaki eksiklik ya da ülke genelindeki yeterli teknik bilgiye sahip deneyimli iç denetçilerin eksikliği nedeniyle istenilen seviyeye ulaşamamıştır. Literatüre baktığımızda konu ile ilgili az sayıda çalışma yapılmıştır. Köse ve Polat yaptıkları çalışmada dijitalleşmenin denetim yöntem ve yaklaşımlarına, denetimin planlanmasına, kanıt toplamaya, uygunluk değerlendirmesine, işlem mutabakatına, bulgu ve önerilere, raporlamaya ve denetim verilerine etkisini değerlendirmişlerdir (Köse & Polat, 2021). Ağdeniz yaptığı çalışmada Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (DDO) tarafından çıkarılan bilgi ve iletişim güvenliği rehberi uyum denetiminde kamu iç denetçilerinin rolü ve yetkinliklerini sertifika ve denetim sayıları temelinde değerlendirmeye çalışmıştır (Ağdeniz, 2021). Akmeşe yaptığı çalışmada karmaşıklaşan teknoloji uygulamaları ile siber saldırıların yöntemlerinin gelişmesi, dağınık bilgi teknolojileri mimarisi, üçüncü taraf hizmet sağlayıcılar ile genişleyen saldırı yüzeyi, siber güvenliğe ilişkin kontrol faaliyetlerinin uçtan uca tüm sistemler ile entegre edilememesi, insan kaynağı yetersizlikleri gibi durumların organizasyonların başarılı bir siber

güvenlik stratejisi uygulamalarını zorlaştırdığını ifade etmiştir. Sürekli gelişen ve değişen teknolojinin getirdiği riskleri yönetmek için iç denetim fonksiyonunun da kendini güncellemesi gerektiği aşikârdır (Akmeşe, 2020). Koç ve arkadaşları BT denetiminde bilgi güvenliği ile ilgili uluslararası standartlardan ve Türkiye'de bilgi güvenliği ile ilgili regülasyonlardan bahsetmişlerdir (Koç v.dğr., 2019). Dutta ve arkadaşları yaptıkları çalışmada organizasyonların fonksiyonlarını yerine getirmesi için çalışanlarına, iş süreçlerine ve teknoloji kullanımına ihtiyaç duyduğunu ve teknoloji kullanımının günümüzde şirket değerini belirlemede önemli bir parametre olduğundan bahsederek BT mimarisini ve süreçlerini, iş süreçlerini ve kullanıcıları göz önünde bulunduran bir BT olgunluk modeli önermiştir (Dutta v.dğr., 2022).

1.1. Problem

BT yönetişimi (Information Technology Governance) organizasyonlara iş hedeflerine ulaşmaları adına BT'de doğru kararların verilmesi ve risklerin yönetilmesi için uygun mekanizmalar sunar (Dutta ve diğerleri., 2022). BT yönetişiminin temelinde ise ulusal/uluslararası standartlar ve ulusal regülasyonlar bulunmaktadır. Denetim elemanları yaptıkları denetimleri bu standartlar ve regülasyonlara dayandırmaktadırlar. Yapılan literatür incelemelerinde uluslararası standartlar ve siber güvenlik konusunda çokça çalışma olmakla beraber ülke regülasyonları hakkında fazlaca çalışma olmadığı görülmüştür. Gerek bu nedenden gerekse Türkiye'de bilişim politikalarına yön veren tekil bir otorite bulunmadığından mütevellit mevzuatın derli toplu olmamasından dolayı zaman zaman kamu zararları da oluşmaktadır. Gerçekleştirilen çalışmada, aşağıdaki sorulara cevap aranmaya çalışılmıştır.

- Kamu idarelerindeki bilgi işlem daire başkanlıkları ya da ilgili genel müdürlüklerde idari açıdan bilişim mevzuatı nelerdir?
- Türkiye'de kamu iç denetimi açısından bakıldığında bilişim mevzuatı nelerdir?
- Türkiye'de kolluk kuvvetleri ve yargı açısından bilişim mevzuatı nelerdir?

1.2. Amaç

Kurumlar dijital dünyada rekabet etmek, müşteri ve vatandaş memnuniyetini sağlayabilmek için yeni dijital iş modellerini ortaya koymakta ve bu dijital teknolojileri organizasyon kültürüne entegre etmeye gayret sarf etmektedirler. İç Denetimin de bu eş güdümde hareket etmesi gereklidir (Görmen ve Korkmaz, 2022). Ancak yukarıdaki varsayımları kanıtlar nitelikte 2008-2019 Kamu İç Denetim Genel Raporları incelendiğinde diğer denetim türlerine kıyasla BT denetimi oransal olarak oldukça azdır. Diğer taraftan, Sertifikalı Bilgi Sistemleri Denetçisi (CISA - Certified Information Systems Auditor) sertifikasına sahip kamu iç denetçisinin sayısı yalnızca 5 (beş) dir (Arkın, 2022). Gerçekleştirilen çalışmada BT denetim sayılarını artırmak adına kamu sektöründe görev yapan BT yöneticileri ile iç denetçilere fayda sağlamak ve literatüre katkı sunmak amacıyla bilgi teknolojilerinin denetimi ile ilgili kamu kurumlarının uyması gereken mevzuatın derlemesi yapılarak kamu iç denetçileri açısından bir denetim kontrol listesi ortaya konulmaktadır.

1.3 Araştırmanın Temel Varsayımları, Sınırlılıkları ve Yöntemi

Çalışma, idari ve yargısal bilişim mevzuatının uygulanmasına dair birkaç varsayım yapılmıştır. Bunlar;

- İç denetim birimlerinde BT konusunda yetkin yeteri kadar iç denetçi bulunmaması.
- İç denetim birimlerinde BT konusunda mevzuatın yeteri kadar bilinmemesi.
- BT birimlerinde BT konusunda yasal ve idari mevzuatın yeteri kadar bilinmediği.

Araştırmada aşağıda belirtilen sınırlıkların mevcudiyeti kabul edilmiştir. Bu kapsamda;

- Çalışmanın yapıldığı tarih itibari ile güncel olan mevzuat değerlendirilmiş olup, mevzuatın daha önceki sürümlerine bakılmamıştır.
- Çalışmada tüm idari ve yargı mevzuatını değil konusu itibari ile BT ile ilişkilendirilebilen kısımlar incelenmiştir.
- Çalışmada ilgili mevzuat BT birim yöneticileri ve iç denetim bakış açısı ile incelenmiştir.
- Çalışmada incelenen mevzuatın dışında her kurumun ve organizasyonun kendi iç yönergeleri, uluslararası mevzuat ve standartlar değerlendirilmemiştir.

Araştırmada nicel olarak yapılmış ve temel olarak tarama yöntemi kullanılmıştır. Çalışmada, evrenin tümü ele alınmış herhangi örneklem alma yoluna gidilmemiştir.

2. YASAL ALTYAPI

Türkiye'ye ilk bilgisayarlar 1960'lardan sonra gelse de yaygın olarak kullanımı 1980'lerden sonra kişisel bilgisayarların ve x86 mimarisine sahip sunucu bilgisayarlarının ortaya çıkması ile olmuştur. Kamu kurumlarında 1990'lı yılların başından itibaren o güne kadar kurum içi uygulamalar amacı ile kullanılan ana bilgisayar sistemleri açık sistem denilen x86 mimariye sahip sunuculara taşınmıştır.

2000'li yılların başında e-Türkiye ve e-dönüşüm projeleri ile beraber iş süreçlerinin sayısallaştırılması hızlanmış ve o zamana kadar yalnızca kurum personeline ve üniversite araştırmacılarına sunulan kurumsal hizmetler internet ortamından vatandaşlara ve diğer paydaşlara sunulmaya başlanmıştır.

Aşağıda bu dönemde dijital dönüşümün yaygınlaştırılması amacı ile gerçekleştirilen bazı çalışmalar sunulmaktadır.

- Dünya Bankası İş Birliği ile Hazırlanan Bilişim ve Ekonomik Modernizasyon Raporu (1993)
- TUBİTAK Ulusal Akademik Ağ ve Bilgi Merkezi (ULAKBİM) 'nin Kurulması (1996)
- Dış Ticaret Müsteşarlığı Bünyesinde Elektronik Ticaret Koordinasyon Kurulu (ETKK) 'nun kurulması (1997)
- Başbakanlığı 1998/13 Sayılı Genelgesi ile Kurulan Kamu-Net Kurulu (1998)
- Ulaştırma Bakanlığı ve TUBİTAK Tarafından Hazırlanan Türkiye Ulusal Enformasyon Altyapısı ve Ana Plan Çalışması (TUEANA) (1999)
- 2002 / 20, 2002 / 55, 2003 / 12, 2003 / 48 Sayılı Başbakanlık Genelgeleri ile Şekillendirilen e-Dönüşüm Türkiye Projesi
- 2018 / 1 Sayılı Cumhurbaşkanlığı Kararnamesi ile Dijital Dönüşüm Ofisi (DDO)'nin Kurulması

Öte yandan; e-dönüşümün hızlanması ile beraber artan uygulama ve sunucu enflasyonunu yönetmek, verilerin bütünlüğünü, güvenliğini ve erişilebilirliğini sağlamak, kişisel verileri korumak, internetin kötüye kullanımını önlemek amacı ile çeşitli standart ve yasalar 1980'li yıllardan itibaren tüm dünyada uygulanmaya başlamıştır.

Son dönemde bilgi teknolojileri, siber güvenlik ulusal bir alan haline gelmiş ve mevcut kanunlara ek olarak bu konuda çok sayıda tebliğ, plan ve rehber yayınlanmıştır. Aşağıda ayrı alt başlıklarda BT ile ilgili mevcut düzenlemeler hakkında kısaca bilgi verilerek değerlendirilmektedir.

2.1. 5237 Sayılı Türk Ceza Kanunu

Bilişim suçları açısından baktığımızda Türkiye'deki ilk yasal mevzuat Türk Ceza Kanunu (TCK)'na 1991 yılında eklenen bilişim sistemine girme, sitemi engelleme ve sistemi bozma suçlarıdır (Kızıltan, 2007). Bu mevzuata ek olarak özel hayata ve gizliliğine karsı suçlar kısmında kişisel verilerin kaydedilmesi, ele geçirilmesi, verilerin yok edilmemesi suçları da bilişim yoluyla işlendiğinden bilişim suçu olarak değerlendirilebilir. TCK'da bilişim ile alakalandırılabilecek diğer suçlar ise hâlihazırda uygulandığı şekliyle organ ticareti, tehdit, taciz, hırsızlık, hakaret, uyuşturucu madde kullanılmasını özendirme, Cumhurbaşkanına hakaret ile devletin egemenlik alametlerini, kurum ve organlarını, cumhuriyeti ve Türklüğü aşağılama olarak sıralanabilir (Akaslan, 2021).

Her ne kadar kamu idareleri açısından yürürlükte olan mevzuatın bir kısmında doğrudan idari ve mali yaptırımlar belirtilmese de bu mevzuatlarda belirtilen tedbirlerin ve faaliyetlerin yerine getirilmediğinde kurum zarara uğruyorsa veya vatandaş ve paydaş zarara uğruyorsa, kasıt ve ihmal yönünden TCK'nın 256. Maddesine göre görevi kötüye kullanma suçu kapsamına girmektedir. Ancak kurumların görevleri net ve açık bir şekilde belirlemesi ve personele doğru şekilde tebliğ etmesi gerekmektedir.

2.2. 5846 Sayılı Fikir ve Sanat Eserleri Kanunu

Ülke mevzuatı tarandığında TCK'dan farklı olarak bilişim suçları ile alakalı karşımıza çıkan bir diğer kanun 5846 sayılı Fikir ve Sanat Eserleri Kanunudur. Kanunda fikri ve sınai bir hak olarak değerlendirilen bilgisayar yazılımlarına ilişkin izinsiz kopyalamalar ve kullanımlara karşı telif hakkı suçları düzenlenmiştir. Buna göre, web sayfaları ve bilgisayar programları dâhil olmak üzere her türlü fikir ve sanat eserini izinsiz olarak kullanan, işleyen, çoğaltan, bilgisayar programlarını koruyan aygıtları geçersiz kılan teknik araçları (keygen ..vb) bulunduran, dağıtan ve izinsiz olarak yayınlayanlar siber suçlu olarak kabul edilmektedir. Buradan hareketle denetim açısından bakıldığında kamu ya da özel

sektör bilgi işlem departmanlarında veya iş birimlerinde kaçak lisanslı ürün kullanılması veya eksik lisans kullanması (örneğin kurumda 2000 personelin kullandığı bir ürünün 250 lisansla satın alınıp geri kalanınca lisanssız kullanımı) kanuna göre suçtur (Arslan, 2022a).

2.3. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" 23.05.2007 tarihinde resmî gazetede yayımlanarak yürürlüğe girmiştir. Kanunla internet ortamındaki içerik üreticileri, yer sağlayıcılar (sunucu ve web sayfası gibi), erişim sağlayıcılar (internet servis sağlayıcılar ya da kurumsal internete çıkış hizmeti veren organizasyonlar) ve toplu kullanım sağlayıcıların sorumluluk ve yükümlülükleriyle internette gerçekleşen suçlarla mücadeleye ilişkin usul ve esaslar düzenlenmiştir. Kanun içerik, yer, erişim ve toplu kullanım sağlayıcılarına çeşitli sorumluluklar yüklemektedir. Buna ek olarak 1 Ekim 2020'de söz konusu kanunda değişiklik yapılarak Türkiye'de yoğun kullanılan sosyal medya devlerinin de suçla mücadeleyi kolaylaştırmak ve hızlandırmak açısından Türkiye de ofis açması istenmiştir.

Erişim sağlayıcı olarak değerlendirildiğinde kamu kurumları ve işletmeler çalışanların ve misafirlerin adli ve idari merciler tarafından istenmesi durumunda herhangi bir kullanıcısının yayınladığı mevzuata aykırı içeriğe erişimi teknik olarak engelleme imkânı bulunduğu ölçüde engellemeli, personelin ve misafirlerin internet trafik bilgisini en az 6 ay en fazla 2 yıl saklamalı ve bu bilgilerin doğruluğunu, bütünlüğünü, gizliliğini sağlamalıdır. Kanunda belirtilen süreler içerisinde mahkemelerden ve savcılıklardan gelen talepleri cevaplamalıdır.

2.4. 6698 Sayılı Kişisel Verilerin Korunması Kanunu

Avrupa Birliği Veri Koruma Tüzüğü (GDPR) ile uyumlu bir şekilde 2016 yılında Türkiye Büyük Millet Meclisinde kabul edilen kanunun temel amacı, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen kişilerin sorumlulukları ve uyacakları esas ve usulleri düzenlemektir. Kanun ile beraber mevzuatı uygulamak amacı ile kurulan Kişisel Verileri Koruma Kurumu özel sektörde olduğu gibi kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarının da aydınlatma, veri güvenliği sağlama, kişisel veri işleme envanteri hazırlama, kişisel veri saklama ve imha politikası hazırlama ve Veri Sorumluları Sicil Bilgi Sistemi (VERBİS)'ne kaydolmalarını yani mevzuata tam anlamıyla 31.12.2021'e kadar uyum sağlamasını istemiştir. Ancak bir istisna olarak kamu kurumlarına Kişisel Verileri Koruma Kurumu (KVKK) tarafından idari para cezası uygulanmamaktadır. Bunun yerine kurum aykırılık tespit ettiğinde disiplin hükümlerine göre sorumlulara gerekli yaptırımların uygulanmasını ilgili kurumlardan istemektedir.

2.5. On Birinci Kalkınma Planı

Kalkınma planları Cumhurbaşkanlığı, bakanlıklar, kamu kurum ve kuruluşları ve çeşitli sivil toplum örgütlerinin katkılarıyla hazırlanmaktadır. Bu planlar devletin temel dokümanlarından biri olarak stratejik planların hazırlanmasında tüm kurumlara önceliklerini belirlemede yön vermektedir. 1963'ten bu yana her 5 yılda bir yayınlanan kalkınma planlarının 2019-2023 yıllarını kapsayan 11.'sinde bilgi ve iletişim teknolojilerinin geliştirilmesi ile kullanımı yoluyla ekonomide rekabet gücünün ve verimliliğin artırılması ve bu suretle iş süreçlerinin dönüştürülmesi temel amacıyla 20 temel tedbir ve politika belirlenmiştir. Bu itibarla kamu kurumlarının hazırladıkları stratejik planlarda ve eylem planlarında kalkınma planı ile eşgüdüm halinde olması gerekmektedir.

2.6. Bilgi ve İletişim Güvenliği Rehberi

Dijital Dönüşüm Ofisi (DDO) 10 Temmuz 2018 tarih ve 30474 sayı ile Resmî Gazete'de duyurulan Cumhurbaşkanlığı Kararnamesi ile kurulmuştur. Söz konusu Kararname ile DDO'ya aşağıdaki görevler verilmiştir;

- Kamu için e-dönüşüm yol haritasını belirlemek,
- Ekosistem oluşturmak için üniversite, kamu ve özel sektör ile sivil toplum kuruluşları arasındaki iş birliğini geliştirerek dijital kamu katılımlarını teşvik etmek,

- Görev alanına giren hususlarda kamu kurumları tarafından hazırlanan yatırım projesi tekliflerine ilişkin Strateji ve Bütçe Başkanlığı'na (Mülga Kalkınma Bakanlığı) görüş vermek ve projelerle ilgili gelişmeleri takip edip gerektiğinde yönlendirmek,
- Bilgi güvenliğini ve siber güvenliği artırıcı çalışmalar yapmak,
- Kamuda büyük veri kullanımına yönelik stratejiler geliştirmek ve eş güdümü sağlamak,
- Kamuda yapay zekâ uygulamalarına yönelik stratejiler geliştirmek ve eş güdümü sağlamak,
- Yerli ve milli dijital teknolojilerin kamuda kullanımının artırılmasını sağlamak,
- Kamu kurum ve kuruluşlarının bilişim ürün ve hizmetlerini maliyet etkin şekilde tedarik etmesine yönelik stratejiler geliştirmek,

Görevleri verilmiştir. Bu çerçevede, 2019/12 sayılı bilgi ve iletişim güvenliği tedbirleri konulu Cumhurbaşkanlığı Genelgesi yayımlanmıştır. Genelge ile kamu kurumları ve kritik altyapı hizmeti veren işletmeler veri güvenliğinin sağlanması amacıyla belirli güvenlik önlemlerini almakla yükümlü kılınmıştır. Genelge 'den sonra 10 Temmuz 2020 tarihinde büyük ölçüde ISO 27001 standardını referans alan Bilgi ve İletişim Güvenliği Rehberi ve bu rehbere göre yapılacak denetimler için de 27 Ekim 2021 tarihinde Bilgi ve İletişim Güvenliği Denetim Rehberi yayınlanmıştır. Rehbere göre kamu kurumları ve kritik altyapı hizmeti veren işletmeler 27.07.2022 tarihine kadar rehbere uyum sağlamalıdır. Rehberin güncel haline göre her yıl yapılması gereken denetimlerin ilkinin 31.12.2022 tarihine kadar tamamlanması gerekmektedir. Rehberde yapılacak denetimlerin öncelikle ilgili kurumun iç denetim birimleri vasıtası ile yapılması, kurumda bilişim teknolojileri (BT) konusunda yetkin denetim elemanı olmaması durumunda ise Türk Standartları Enstitüsü (TSE)'nün "Bilgi ve İletişim Güvenliği Rehberi Uyum Denetimi Hizmeti Sağlayan Personel ve Firma Belgelendirmesi" programı kapsamında belgelendirilmiş denetmen ve firmalardan hizmet alınması regüle edilmiştir. Ancak rehberde tamamlanmayan denetimler ve karşılaşılan uyum eksiklikleri konusunda kurumlara herhangi bir yaptırım öngörülmemiştir.

2.7. 2020-2023 Ulusal Siber Güvenlik Strateji Belgesi

20/10/2012 tarih, 28447 sayılı Resmi Gazetede yayınlanan Bakanlar Kurulu Kararı ve 5809 sayılı Elektronik Haberleşme Kanunu gereğince ulusal siber güvenliğin sağlanmasına ilişkin strateji, politika ve eylem planlarını hazırlamak ve gerekli eş güdümü sağlama görevi Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'na (sonrasında ismi Ulaştırma ve Altyapı Bakanlığı olarak değişti) verilmiştir.

Türkiye'de siber güvenlik alanında ilk temel mevzuat olan "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı", 20 Haziran 2013 tarih ve 28683 sayılı Resmî Gazete' de yayımlanarak yürürlüğe girmiştir. Devamında 2016-2019, 2020-2023 olarak iki kez güncellenmiştir. Bununla beraber 27 Ocak 2000 tarih ve 4502 sayılı Kanun ile "Telekomünikasyon Kurumu" adıyla kurulan ve daha sonra 809 sayılı ve 10 Kasım 2008 tarihli Elektronik Haberleşme Kanunu ile adı Bilgi Teknolojileri ve İletişim Kurumu olarak değiştirilen BTK'ya 15 Ağustos 2016 tarihinde 5809 sayılı Elektronik Haberleşme Kanunu'na eklenen hükümler ile siber saldırıların engellenmesi ve caydırıcılığın sağlanması görevleri verilmiştir. Yine aynı kanunla yükümlülüklerini yerine getirmeyen taraflara yaptırım uygulama yetkisi de BTK'ya verilmiştir. Ancak Cumhurbaşkanlığı hükümet sistemine geçilmesi ve DDO'nun kurulması ile beraber Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, BTK ve DDO arasında siber güvenlik otoritesi olma noktasında bir görev çakışması bulunmaktadır.

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, Türkiye'nin siber güvenlik alanındaki vizyon ve misyonu doğrultusunda 4'er yıllık dönemlere ilişkin politikalarını konu almaktadır. Bu çerçevede, son yayınlanan planda belirlenen stratejik amaçlar aşağıda sıralanmıştır;

- Kritik Altyapıların Korunması ve Dayanıklılığının Artırılması
- Ulusal Siber Güvenlik Kapasitesinin Artırılması
- Organik Siber Güvenlik Ağı
- Yeni Nesil Teknolojilerin Güvenliğinin Sağlanması
- Siber Suçlarla Mücadelenin Etin Bir Şekilde Sağlanması
- Siber Güvenlik Alanında Yerli ve Milli Teknolojilerin Geliştirilmesi ve Desteklenmesi
- Siber Güvenliğin Milli Güvenliğe Entegrasyonunun Sağlanması
- Siber Güvenlik Alanında Uluslararası İş Birliğinin Geliştirilmesi

Plana göre gerçekleştirilmesi hedeflenen toplam 8 adet stratejik amaçla ilişkilendirilen 40 adet eylem ve bunlarla ilişkili 75 adet uygulama adımı vardır.

2.8. KamuNet Ağına Bağlanma ve KamuNet Ağının Denetimine İlişkin Usul ve Esaslar Tebliğ

Kamu kurum ve kuruluşları arasında ihtiyaç duyulan veri iletişiminin, güvenli ağ üzerinden yapılarak siber güvenlik risklerinin azaltılması amacıyla oluşturulmuş KamuNet tebliği 21 Haziran 2017 Tarih ve 30103 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiştir. Tebliğ KamuNet'e dâhil edilecek ve dâhil olan kamu kurumlarının veri merkezlerinde karşılaması gereken asgari gereklilikler ile bu kurumların denetlenmesine ilişkin usul ve esasları belirlemektedir. Söz konusu mevzuata uyum sağlanması için kamu kurumlarının bir Bilgi Güvenliği Yönetim Sistemi (BGYS) sistemi kurması gerekmektedir. Tebliğde ISO 27001 sertifikası alımını dahil olmak üzere bir dizi siber güvenlik tedbiri alınmasını zorunlu kılınmıştır. Denetimlerin ise periyodik sürelerde Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından yapılacağı ifade edilmiştir. Ancak mevzuatta periyodik denetimlerde tespit edilen eksiklikleri gidermeyen kamu kurumlarının KamuNet erişimini askıya alınır veya çıkarılır denmesine rağmen şu ana kadar söz konusu denetimlerin yapılıp yapılmadığına ya da denetimlerin sonuçlarına dair bakanlık tarafından herhangi bir geri bildirim kamuoyu ile paylaşılmamıştır.

2.9. Lisanslı Yazılım Kullanımına Dair Başbakanlık Genelgesi

16 Temmuz 2008 Tarih ve 26938 sayılı Başbakanlık Genelgesinde 5856 Sayılı Fikir ve Sanat Eserleri Kanuna atıf yapılarak, fikri hakların korunması açısından, kamu kurum ve kuruluşlarında, bilgisayar programlarının edinilmesi, kullanılması, yönetimi ve alınacak tedbirlere yönelik esasların tespiti ile ilgili düzenlemeler yapılmıştır. Buna göre; lisans hakları kamu kurum ve kuruluşuna ait olmayan tüm programların medya ve bilgisayarlardan silinmesi ve lisanslı olanların alınması istenilmiştir. Yine aynı tebliğde bu konunun denetiminin kamu kurum ve kuruluşunda bilgi işlem ünitesi veya bu işten sorumlu birimin eş güdümünde hukuk müşavirliğiyle teftiş veya denetiminden sorumlu kurul veya birimlerin ortak veya ayrı ayrı çalışması sonucu tamamlanması istenmiştir. Ancak yapılan mevzuat ve olay taramasında kamu kurumlarında bu konuya ilişkin örnek bir karara veya disiplin soruşturmasına rastlanmamıştır.

2.10. Ulusal Siber Olaylara Müdahale Merkezi (USOM) ve Sektörel SOME'ler

Bölüm 2.7'de de bahsedildiği gibi BTK siber saldırıların engellenmesi ve caydırıcılığın sağlanması amacı ile gerekli önlemleri almak, mevzuata uymayan, belirtilen tedbirleri yerine getirmeyen taraflara yaptırım uygulamakla sorumludur. Öte yandan 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunu'nun 10. maddesi ile 5809 sayılı Elektronik Haberleşme Kanunu'na benzer şekilde BTK'ya siber saldırıların tespiti ve önlenmesi konusunda yer, içerik, erişim sağlayıcılar ve ilgili diğer kurum ve kuruluşlarla koordinasyon sağlama, ihtiyaç duyulan önlemlerin alınması ve aldırılması konusunda çalışmaları yürütme yetkisi verilmiştir.

2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planında da öngörüldüğü şekilde 11 Kasım 2013 tarih ve 28818 Sayılı "Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ" Resmî Gazete'de yayımlanarak yürürlüğe girmiştir. Kanunun yürürlüğe girmesinden sonra Ulusal Siber Olaylara Müdahale Merkezi (USOM) siber güvenlik ile ilgili tehditler ve alınacak önlemlere ilişkin ulusal ve uluslararası çalışmalar yapmak için BTK bünyesinde kurulmuştur. Kanunla beraber Siber Olaylara Müdahale Ekiplerinin (SOME) kamuda, kritik sektörler ile bu sektörleri düzenlemek ve denetlemekten sorumlu kurumlar bünyesinde kurulması istenmiştir. Kurumsal SOME'ler, siber olayların engellenmesi ve(ya) zararlarının azaltılmasına yönelik olarak kurumların bilişim sistemlerinin kurulması, geliştirilmesi işletilmesi ve siber güvenlik farkındalığının oluşması ile ilgili çalışmalar yapmak varsa birlikte çalıştığı sektörel SOME ile eş güdüm içerisinde siber olayları USOM'a bildirmekle sorumludurlar.

2.11. Türkiye'nin Taraf Olduğu Uluslararası Sözleşmeler

Türkiye, Avrupa Konseyi'nin 23.11.2001'de imzaya açtığı Siber Suçlar Sözleşmesini (Budapeşte Sözleşmesi de denir) 10.11.2010'da imzalamış ve devamında 02.05.2014 tarihinde yürürlüğe koymuştur. Aliusta ve Benzer yaptıkları çalışmada sözleşmeyi ve Türkiye'nin dahil olma sürecini detaylı olarak ele almışlardır (Aliusta & Benzer, 2018).

Sözleşmede özetle bilişim suçlarıyla ilgili taraf devletlerin mevzuatlarını uyumlu hale getirerek uluslararası adli yardım ve iş birliği konusunda etkili ve hızlı bir sistem oluşturmak amaçlanmıştır.

Türkiye'nin bilişim alanında taraf olduğu bir diğer uluslararası sözleşme, fikri hakların dünya çapında korunmasını sağlamayı amaçlayan Dünya Fikri Mülkiyet Örgütü (WIPO-World Intellectual Property Organization)' dür. Türkiye 12 Mayıs 1976 tarihinde imzaladığı kuruluş sözleşmesi ile beraber toplamda imzaladığı 15 sözleşme ile örgüte taraftır.

2.12. Başsavcılıklar Bünyesinde Kurulan Bilişim Suçları Soruşturma Büroları ve Bilişim İhtisas Mahkemeleri

Bugüne kadar Adalet Bakanlığına bağlı 145 Ağır Ceza Mahkemesi ve Cumhuriyet Başsavcılığında Bilişim suçları büroları kurulmuştur (Bilişim Suçları Değerlendirme Toplantısı, 2022). Mevcut işleyişe göre Hakimler ve Savcılar Kurulu (HSK) tarafından Bilişim Suçları Soruşturma Bürolarına Bilişim Suçları Savcıları atanmakta ve bilişim sistemleri yoluyla işlenen suçlar değerlendirilmektedir. Öte yandan Türkiye'de bilişim ihtisas mahkemeleri 15.12.2021 tarihinden itibaren hizmet vermeye başlamıştır. HSK'nın 25 Kasım 2021 tarih ve 1229 numaralı kararına göre bu mahkemeler Türk Ceza Kanunu'nun bilişim suçları kapsamına giren konuları ile 29.04.1959 tarih ve 7258 sayılı "Futbol ve Diğer Spor Müsabakalarında Bahis ve Şans Oyunları Düzenlenmesi Hakkında Kanun" kapsamındaki davalara bakmaktadırlar.

2.13. Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Dairesi

2011/2025 sayılı Bakanlar Kurulu Kararı ile Emniyet Genel Müdürlüğü bünyesinde Siber Suçlarla Mücadele Daire Başkanlığı kurulmuştur. Daire, Elektronik Haberleşme Kanunu, Türk Ceza Kanunu'nun bilişimle ilgili maddeleri, Fikir ve Sanat Eserleri Kanunu ile Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına yönelik ilgili yönetmelikler gereğince işlem tesis etmektedir.

Dairenin genel olarak görev alanında bilişim ve internet alanını içerisinde gerçekleştirilen e-mail ve sosyal medya adreslerinin çalınması, kredi kartı bilgilerinin ele geçirilmesi vasıtası ile hırsızlık, sahte evraklar düzeyerek dolandırıcılık, kişisel ve kurumsal verilere yetkisiz erişim ve iletişimin yetkisiz dinlemesi, yazılımların izinsiz ve lisanssız kullanımı, çocuk pornografisi ve istismarı, hakaret ve tehdit, uyuşturucu kaçakçılığı, siber terör gibi konular bulunmaktadır.

2.14. Adli Tıp Bünyesinde Kurulan Adli Bilişim İhtisas Dairesi

01.09.2016 tarih ve 674 sayılı Kanun Hükmünde Kararname (KHK) ile 14.4.1982 tarih ve 2659 sayılı Adlî Tıp Kurumu Kanununa ek yapılmış ve kurum bünyesinde Adli Bilişim İhtisas Dairesi kurulmuştur. Dairenin görevleri ise mahkemeler ile hâkim ve savcılıklar tarafından istenilen bilişimle ilgili konularda her türlü sayısal ve elektronik materyal üzerinde analiz ve incelemeleri yapmak olarak belirlenmiştir.

2.15. Adalet Bakanlığı Bilirkişilik Daire Başkanlığı

03.11.2016 tarih ve 6754 sayılı Bilirkişilik Kanunu, 24.11.2016 tarih ve 29898 sayılı Resmî Gazetede yayımlanmıştır. Bu Kanun kapsamında bilirkişilik hizmetlerinin etkin, etkili ve verimli şekilde gerçekleşmesini sağlamak için Adalet Bakanlığı Hukuk İşleri Genel Müdürlüğü bünyesinde "Bilirkişilik Daire Başkanlığı" kurulmuştur.

Mahkemeler, bilişim davaları ile ilgili konularda Türkiye'de 15 adet bulunan bilirkişilik bölge kurullarından hangisinin bölgesine giriyor ise o bölgenin bilirkişi listesinden uzman görevlendirmesi yapabilirler.

3. DENETİM KONTROL LİSTESİ

Yukarıda bahsedilen yasal mevzuat ve düzenlemelerin değerlendirilmesi sonucunda bilgi işlem birimlerinde BT denetimi yapacak olan iç denetim birimleri ve iç denetçilere izleyebilecekleri yol haritası örneği olması amacıyla toplam yedi kategoride hazırlanan soru seti aşağıda Tablo-1' de sunulmuştur.

Tablo 1. İç Denetçiler İçin Soru Seti

6698 Sayılı Kanununa Uyum	Veri Sorumluları belirlenmiş midir?
	Kurum içerisindeki veri tabanlarında ve dokümanlarda bulunan kişisel veriler tespit edilmiş midir?
	Veriyi işleyen personeller belirlenmiş midir?
	VERBİS'e kaydedilmiş ve güncel midir?
	Sürdürülebilir güncel bir sistem kurulmuş mudur?
	Kurumda zorunlu olmayan ya da kanuni tutma süresi biten kişisel verilerin silinmesine yönelik bir sistem var mıdır?

	Vatandaştan alınan kişisel verilerin gizlenmesi ya da silinmesine yönelik dilekçelerin işlenmesine ve yerine getirilmesine yönelik tüm uygulamaları içeren bir sistematik kurulmuş mudur?
	Diğer kamu kurumları ile veri paylaşımları yapılıyor mu? Yapılıyor ise bir listesi tutuluyor mudur?
	Veri paylaşımları kurumlar arası yapılan protokollere dayanıyor mu? Protokollerin süresinin kontrolü ile ilgili olarak bir sistematik var mıdır?
5651 Sayılı Kanuna Uyum	Kablolu ağlardan sisteme katılan personelin internete çıkışları zaman damgalı bir şekilde loglanıyor mudur?
	Kablosuz ağlardan sisteme katılan personelin internete çıkışları zaman damgalı loglanıyor mudur?
	Kablosuz ağlardan sisteme katılan misafirlerin internete çıkışları zaman damgalı loglanıyor mudur?
	Kurumun sunduğu portallara, web ve mobil uygulamalara erişenler kayıt altına alınıyor mudur?
	Kayıtlar kanunda belirtilen süreler dâhilinde saklanıyor mudur?
	Savcılık, mahkeme, teftiş kurulları ve iç denetim birimlerinden gelen taleplere kanuna göre uygun cevaplar veriliyor mudur?
USOM ve SOME İlkelerine Uyum	Personelin ve bilişim sistem yöneticilerinin karşılaşacakları siber olayları bildirdikleri bir SOME ekibi oluşturulmuş mudu?
	Resmi olarak ekip üyelerine ve personele bildirilmiş midir?
	SOME ekibi rutin olarak toplanıp siber olayları değerlendiriyor mu? Toplantı tutanakları tutulmuş mudur?
	SOME ekibi tespit edilen zafiyet ve saldırıları USOM'a formal bir şekilde iletiyor mudur?
	USOM'dan gelen bildirimleri SOME ekibi formal bir şekilde ilgililere iletiyor mudur?
5846 Sayılı Kanununa ve 26938 Sayılı Genelgeye Uyum	Kurumda kullanılan tüm yazılım ve donanım ürünlerinin envanteri tutulmuş mu ve güncelliği sistematik olarak sağlanıyor mudur?
	Kurumun kendi geliştirdiği yazılımlar dışında dışarıdan satın aldığı yazılım ve lisans gerektiren donanım (appliance) ürünlerinin lisansı satın alınmış mıdır?
	Kurumun kendi geliştirdiği yazılımlar dışında dışarıdan satın aldığı yazılım ve lisans gerektiren donanım (appliance) ürünlerinin lisansı güncel midir?
	Kurumun kendi geliştirdiği yazılımlar dışında dışarıdan satın aldığı yazılım ve lisans gerektiren donanım (appliance) ürünlerinin lisansı kullanıcı sayısı, kullanılan CPU vb lisans parametreleri ile uyumlu mudur?
Bilgi ve İletişim Güvenliği Rehberine Uyum	Kurumda bir varlık envanteri çıkarılmış mıdır?
	Envanterler için bir risk hesaplaması yapılmış mıdır?
	Boşluk analizi yapılmış mıdır?
	1, 2 ve 3. seviye tedbirlerin yerine getirilmesi için bir eylem planı yapılmış mıdır?
	Her yıl düzenli bir şekilde İç Denetim Birimlerine ya da Dış Denetim birimlerine uyum denetimi yaptırılmış mıdır?
	Denetim bulguları sonucu ortaya çıkan eksikliklerle ilgili sistematik bir eylem planı yönetimi yapılıyor mudur?
KamuNET Genelgesine Uyum	Kurum KamuNET sistemine bağlı mıdır?
	Hangi uygulamalar KamuNET üzerinden hizmet vermekte belirli midir?
	KamuNET Genelgesine uygun şekilde siber güvenlik önlemleri alınmış mıdır?
	İnternet Hizmeti KamuNET genelgesi kapsamında indirimli tarifeden ilgili ISP'ye ödeniyor mudur?
5237 sayılı Kanuna Uyum	Kurumda tüm bilişim organizasyonunun yapısı net ve anlaşılır bir şekilde tanımlanmış mıdır?
	Tüm bilişim ve diğer iş birimi personellerinin görev ve sorumlulukları belli midir?
	Tüm personellerinin görev ve sorumlulukları kendilerine resmi olarak iletilmiş, imzalatılmış ve personel özlük dosyasına konulmuş mudur?
	Görevi kötüye kullanan ve suiistimal eden personellere yönelik yapılacak adli idari soruşturmalar konusunda bir akış çıkarılmış mı? ve tüm personellere duyurulmuş mudur?

(Araştırmacılar Tarafından Geliştirilmiştir)

3.1. Tartışma ve Öneriler

İç denetçilerin bilişim denetimi konusunda yetkinliklerinin artırılması kamu kurumlarının bilişim mevzuatına uyumunu sağlamak açısından önemlidir. Gerçekleştirilen bu çalışmada, 2000'li yılların başından bugüne Türk kamu idarelerinin dijital dönüşümüne öncülük eden dokümanlar ile dağınık vaziyette çeşitli yönetmelik ve yasalar içerisinde bulunan bilişim mevzuatı tespit edilerek değerlendirilmiştir. Yapılan incelemede Cumhurbaşkanlığı hükümet sistemi ve devamında kurulan DDO ile beraber çeşitli görev çakışmalarının ortaya çıktığı gözlemlenmiştir. Özellikle Ulaştırma ve Altyapı Bakanlığı (UAB), BTK ve DDO arasında bulunan bu görev çakışmalarının izleme ve denetim açısından sorunlara yol açabileceği değerlendirilmektedir.

DDO bilgi ve iletişim güvenliği rehberinde mevzuatın herhangi bir yaptırımının olmaması idarelerin uyum motivasyonunu düşürebilir. Ortaya konan mevzuatın (kamu ihale süreçleri de gözetilerek) gerçekleştirilmesinin

izlenmemesi ve yaptırımının olmaması zımni olarak mevzuata uyan idareleri ve idarecileri cezalandırmak anlamına gelebileceği unutulmamalıdır.

Özellikle bilişim ve siber güvenlik yatırımları halihazırda büyük oranda ithalata bağlıdır. Bu nedenle kamu kurumlarına herhangi bir mevzuata uyum için sorumluluk verilirken, kurumların mevzuata uyum için yapacağı yatırımlarla ilgili ödeneklerin de sağlanması gerekmektedir.

5651 ve 6698 sayılı yasalar ile kurumlarla ilgili münhasır yasalar dikkate alınarak toplanan kişisel verilerin en fazla ve en az ne kadar süre tutulabileceği konusu üst yönetim ve ilgili diğer birimler tarafından tartışılarak netleştirilmelidir.

Denetim elemanlarınca gerçekleştirilen denetimlerde WIPO sözleşmelerine ülke olarak taraf olunduğundan, 16 Temmuz 2008 Tarih ve 26938 sayılı "Lisanslı Yazılım Kullanımına Dair Başbakanlık Genelgesi"ni de dikkate alarak lisanssız ve kaçak ürün kullanıp kullanılmadığının denetlenmesi gerekmektedir. Bu konuda farkındalığın artırılması ve Başbakanlık mülga olduğundan ilgili mevzuatın Cumhurbaşkanlığınca güncellenerek yeniden yayınlanmasında fayda bulunmaktadır.

4. SONUÇ

Çalışmada BT yöneticileri, bilişim mevzuatını denetlemekle sorumlu olan iç denetim birimleri ve iç denetçiler için bir denetim kontrol seti hazırlanmıştır. Hazırlanan soru setleri yalnızca mevzuata uyum açısından hazırlanmış olup bununla beraber denetimlerde ISO20000, ISO 27001, ISO 9001, ISO 14001, ISO 22237, BICSI 002, ISO 38500, ISO 22301, ISO 17799, ITIL, TOGAF, CMMI, COBIT gibi uluslararası bilişim standartlarını merkeze alan özel denetimler de yapılması mümkündür. Bununla beraber denetçilerin denetime başlamadan önce kurum faaliyet alanı, vizyon, misyon, kurum stratejik planı, servis kataloğu, performans programı, faaliyet raporu ve eylem planları kurum organizasyon yapısı, bilgi işlem biriminin organizasyondaki yeri ve sorumlulukları, kurum dış paydaşları ve protokollerini de incelemesinde fayda bulunmaktadır (Arslan, 2022b).

DDO tarafından ortaya konan Bilgi ve İletişim Güvenliği Rehberi'yle kapsamdaki tüm kurumlarda denetimlerin öncelikli olarak iç denetim birimlerindeki iç denetçiler tarafından gerçekleştirilmesinin esas olduğunun ifade edilmesi iç denetçiler açısından çok faydalı olmuştur. Bu itibarla birçok iç denetçi Kamu İç Denetim Derneği (KİDDER) gibi kuruluşların verdiği BT denetim eğitimlerini alarak denetime hazır hale gelmiştir.

Kamuda BT denetimlerini yapan iç denetçiler açısından konu değerlendirildiğinde kamu idarelerinde büyük oranda boş iç denetim kadrolarının olduğu görülmektedir. Kamu iç denetim kadrolarının daha da artırılarak açık bulunan kadrolara atama yapılması ve iç denetçilerin bilişim denetimi konusunda yetkinliklerinin artırılması kamu kurumlarının bilişim mevzuatına uyumunu sağlamak açısından önemlidir. Denetimler sırasında iç denetçiler; uluslararası metodolojiye uygun şekilde kişilere değil sürece odaklanmalı, hatayı kimin yaptığını değil süreç içerisinde bu hatanın yapılmasına neden olan bilişim süreç eksikliğini sorgulamalı, iyi uygulama örneklerinin altını çizerek idarecileri motive etmeli ve kurumlarda sürdürülebilir bir bilişim yönetim sisteminin kurulumuna öncülük etmelidirler.

Kaynakça

Ağdeniz, Ş. (2021). Bilgi ve iletişim güvenliği denetiminde kamu iç denetçilerinin rolü ve yetkinliklerine ilişkin bir araştırma., *Alanya Akademik Bakış, 5*(2), 525-545.

Akaslan, N. M., (2021). Yeni bir ihtisas mahkemesi olarak bilişim mahkemesi., https://www.hukukihaber.net/yeni-bir-ihtisas-mahkemesi-olarak-bilisim-mahkemesi-makale,8797.html (Erişim Tarihi, 08.03.2022)

Akmeşe, S. (2020). Kamuda dijital dönüşümün siber güvenlik ve dijital güvence boyutları ve iç denetimin rolü. *Denetişim Dergisi*, *0* (20), 108-119.

Aliusta, C. & Benzer, R. (2018). Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dâhil Olma Süreci., *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 4(2), 35-42.

Arkın, A. (2022). Kamu iç denetim genel raporlarının içerik analizi, *Denetişim Dergisi*, 0 (25), 27-57.

Arslan, Y. (2022a). Bilişim suçları ve bilirkişilik mesleği., https://ictmedia.com.tr/Author/Index/55/dr-yenal-arslan/646 (Erişim Tarihi, 15.05.2022).

Arslan, Y. (2022b). Bilgi ve iletişim güvenliği rehberi uyum denetimi., https://ictmedia.com.tr/Author/Index/55/dr-yenal-arslan/646 (Erişim Tarihi, 15.05.2022).

Bilişim Suçları Değerlendirme Toplantısı (2022), https://cigm.adalet.gov.tr/Home/SayfaDetay/Antalya05122022 (Erişim Tarihi, 15.10.2022).

COSO. (2019). *Enterprise Wide Management (ERM) for Cybersecurity*. https:// www.coso.org/Documents/COSO-Deloitte-Managing-Cyber-Risk-in-a-Digital-Age.pdf (Erişim Tarihi, 16.05.2020).

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (2019). *Bilgi ve İletişim Güvenliği Denetim Rehberi*. Ankara.

Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı. (2019). *On Birinci Kalkınma Planı*. Ankara.

Deloitte. (2017). *Deloitte's Cyber Risk Capabilities, Cyber Strategy, Secure, Vigilant, and Resilient*. https://www2.deloitte.com/content/dam/Deloitte/at/Documents/risk/cyber-risk/Deloitte-Cyber-Risk-Capabilities-Broschuere.pdf (Erişim Tarihi, 15.04.2022).

Dutta, A., Roy, R. & Seetharaman, P. (2022). An assimilation maturity model for IT governance and auditing., *Information & Management*, 59(1), 1-21.

ECIIA. (2020). *Risk in Focus 2021. Hot Topics for Internal Auditors*. https://www.eciia.eu/wp-content/uploads/2020/09/100242-RISK-IN-FOCUS-2021-52PP-ECIIA-Online-V2.pdf (Erişim Tarihi, 20.04.2022).

FERMA. (2019). *At The Junction of Corporate Governance & Cybersecurity*. https://www.eciia.eu/wp-content/uploads/ 2019/02/FERMA-Perspectives-Cyber-risk-governance-09.10.2018_0.pdf (Erişim Tarihi, 16.03.2022).

George, D., Theofanis, K. & Konstantinos, A. (2015). Factors associated with Internal Audit Effectiveness: Evidence from Greece. *Journal of Accounting and Taxation*, 7(7), 113-122.

Görmen, M. & Korkmaz, G. (2022). Kurumsal Sürdürülebilirlik İçin Sürdürülebilir İç Denetim: Geleceğin İç Denetim Fonksiyonu, *Denetişim Dergisi*, 0 (25), 94-115.

IIA. (2013). *The Three Lines of Defence in Effective Risk Management and Control*. https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf (Erişim Tarihi, 20.03.2022).

IIA. (2016). *Assessing Cybersecurity Risk: Roles of the Three Lines of Defense*. https://global.theiia.org/standards-guidance/Member%20Documents/ GTAG-Assessing-Cybersecurity-Risk.pdf (Erişim Tarihi, 05.03.2022).

IIA. (2020). *On Risk2022. A Guide to Understanding, Aligning, and Optimizing Risk*. http://theiia.mkt5790.com/OnRisk2020/webSyncID=9d4b5b56-2d9e-c43b83c5b525&sessionGUID=d03ed4d7-83b6-86b2-406b-326988476708 (Erişim Tarihi, 20.05.2022).

İç Denetim Koordinasyon Kurulu. (2021). *2020 Yılı Kamu İç Denetim Genel Raporu*. Ankara.

Koç, S., Şeker, S. & Şeker, F. (2019). Bilişim teknolojileri (BT) denetiminde bilgi güvenliği ile ilgili uluslararası standartlar ve Türkiye'deki uyum çabalarının incelenmesi., *Muhasebe ve Finans Araştırmaları Dergisi*. 1(2), 121-139.

Köse, H. Ö. & Polat, N. (2022). Dijital dönüşüm ve denetimin geleceğine etkisi., *Sayıştay Dergisi*, 32(123), 9-4.

M., B., Kızıltan. (2007). *5237 Sayılı Türk Ceza Kanununda Bilişim Sistemine Girme, Sistemi Engelleme ve Bozma Suçları*, (Basılmamış yüksek lisans tezi), İstanbul Üniversitesi, İstanbul.

Moore, R. (2005). *Cyber crime: Investigating High-Technology Computer Crime*. Mississippi: Anderson Publishing.

NIST. (2013). "*Special Publication 800-53, Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations*". USA.

Özbilger, H.İ. (2021). İç denetime yeni bir bakış: Üçlü hat modelinin değerlendirilmesi., *Denetişim Dergisi,* 0 (22), 40-54.

Stoel, D., Havelka, D. & Merhout, J.W. (2012). An analysis of attributes that impact information technology audit quality: A study of IT and financial audit practitioners., *International Journal of Accounting Information Systems*, 13(1), 60–79.

Turetken, O., Jethefer, S., Ozkan, B., (2020). Internal audit effectiveness: Operationalization and influencing factors. *Managerial Audit*. 35(2), 238–271. https://www.emerald.com/insight/content/doi/10.1108/MAJ-08-2018-1980/full/html (Erişim Tarihi, 19.03.2022).

Ulaştırma ve Altyapı Bakanlığı. (2020). *Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020–2023).* Ankara.

Ulaştırma Denizcilik ve Haberleşme Bakanlığı. (2016*). Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2016–2019).* Ankara.

HAKEMLİ Denetişim
Ortak Aklın Harmanı

Kamu İç Denetçileri Derneği Meşrutiyet Caddesi Konur Sokak No: 36/6 Kızılay - ANKARA
www.kidder.org.tr/denetisim/ • denetisim@kidder.org.tr
ISSN 1308-8335
Yıl: 13, Sayı: 26,13-31, 2022

Araştırma Makalesi

DENETİMDE TEKNOLOJİK GELİŞMELERİN DENETİM SÜRECİNE OLAN ETKİLERİNİN AKADEMİSYEN GÖRÜŞLERİYLE İNCELENMESİ

(EXAMINATION OF THE EFFECTS OF TECHNOLOGICAL DEVELOPMENTS TO AUDITING ON THE AUDIT PROCESS WITH THE OPINIONS OF ACADEMICIANS)

Nazan GÜNGÖR KARYAĞDI[1]

Öz

Çalışmanın amacı güncel yaklaşımlara bağlı olarak gelişen teknolojiler ve yaşanan dijitalleşme sürecinin denetime ve denetim sürecine olan etkilerinin araştırılması; denetim alanında akademik çalışmalar yapan akademisyenlerin konuya ilişkin görüşlerinin değerlendirilmesidir. Çalışma grubu ölçüt örneklem yöntemi kullanılarak denetim alanında çalışma yapan 14 akademisyenden oluşmaktadır. Çalışma nitel bir araştırma olup; görüşme tekniği kullanılmıştır. Elde edilen veriler yarı yapılandırılmış görüşme formu tekniği kullanılarak toplanmıştır. Verileri açıklayan temaların belirlenmesi amacıyla da içerik analizi kullanılmış ve doğrudan alıntılara yer verilmiştir. Çalışma sonucunda kullanılan yaklaşım ve teknolojik gelişmelerin denetim süresini kısaltarak gerek denetim kalitesine gerekse verimliliğine olumlu etkisinin olduğu; istihdama ise olumsuz etkisinin olacağı buna karşın denetçilerin kendilerini sürekli yenilemelerinin kaçınılmaz olduğu, pandemi sürecinde ortaya çıkan uzaktan çalışma sisteminin ise sürece olumsuz yansıdığı, teknolojik gelişmelerin denetim alanında kullanılmasıyla risk değerlendirmelerinin daha doğru yapılabileceği yönünde sonuçlar elde edilmiştir.

Anahtar Kelimeler: Dijitalleşme, Denetim, Denetim Süreci ve Akademisyen

JEL Kodları: M15, M4

Abstract

The aim of the study is to investigate the effects of developing technologies and digitalization process on audit and audit process depending on current approaches; to evaluate the opinions of academicians doing academic studies in the field of audit on the subject. The working group consists of 14 academicians working in the field of auditing using the criterion sampling method. The study is a qualitative research and interview technique was used. The data obtained were collected using the semi-structured interview form technique. In order to determine the themes explaining the data, content analysis was also used and direct quotations were included. As a result of technological advances and approaches that are used in the study of the positive impact on Audit Quality and audit efficiency to shorten the duration of the need is that will have a negative impact on employment, however, the auditors of constantly renew themselves is inevitable, reflects the process of remote working system arising in the process of the pandemic, and technological developments in the field of auditing can be made more accurate through the use of risk assessments in the direction of where the results were obtained.

Keywords: Digitalization, Audit, Audit Process and Academician

JeL Classification: M15, M4

[1] Dr. , Bitlis Eren Üniversitesi Sosyal Bilimler Meslek Yüksekokulu Muhasebe ve Vergi Uygulamaları Bölümü, Orcid Id: 0000-0003-3938-4147, ngkaryagdi@beu.edu.tr

1. GİRİŞ

Son yıllarda yaşanan gelişmeler ile özellikle bilginin hızlı elde edilmesi, saklanması, düzenlenmesi ve sunulması açısından birçok alanda önemli düzeyde dönüşüm sağlanmıştır. Bilişim teknolojilerinde değişim ve gelişmelerin hızlı yaşandığı bu süreçte kamu ve özel işletmeler tarafından yürütülen denetim faaliyetleri elektronik ortamda yapılmaya başlanmıştır. Bu gelişmeler, büyük bir öneme sahip olan denetim sistemine ve uygulamalarına yansımıştır. Küreselleşmeyle birlikte ortaya çıkan rekabete bağlı olarak bu değişim ve dönüşüme uyum sağlamak işletmeler için kaçınılmaz bir hal almıştır. Hız kazanan dijitalleşmeyle birlikte yapay zekâ, bulut teknolojisi, nesnelerin interneti, veri analitiği ve büyük veri, blok zincir, akıllı sözleşmeler gibi bir çok teknolojik yenilik ortaya çıkmış ve bu süreç bazı kaynaklarda "Sanayi 4.0, Endüsrti 4.0" ve denetim alanında ise " Denetim 4.0" gibi isimlerle ifade edilmeye başlanmıştır. Gelişen teknolojinin ve dijitalleşmenin etkisiyle kurum ve kuruluşların denetime olan ihtiyaçları artmış, faaliyetlerin gerçekleştirilmesinde farklı teknik ve yöntemlerin kullanılmasına zemin hazırlamıştır.

Dijital değişim ve dönüşümün bir seçimden çok artık bir zorunluluk olduğu gerçeği ortaya çıkmış; bütün mesleklerde olduğu gibi denetim mesleğini icra eden ya da denetimle ilgilenen diğer kesimler tarafından da dijital değişim ve dönüşüm benimsenmeye başlanmıştır. Böylelikle yirmi yıl öncesinde yapılan denetim faaliyetlerinde çalışma kâğıtlarının elle yazılması gibi eski yöntemler bilgisayar kullanımının hız kazanmasıyla geride kalmış; veri kullanımı, kaydı, işlemleri yapma, koordine etme, paylaşma, iletişim kurma gibi birçok işlem de daha kolay ve aktif bir şekilde yapılmaya başlanmıştır. İnsansız ve ışıksız ortamlarda aktif bir şekilde faaliyet gösterecek robotların tasarlanması beraberinde üretimin artması, hataların daha aza indirilmesi ve verimliliğin arttırılması gibi fırsatları getirmiştir. Bunun yanı sıra, verilerin izlenmesinde süreçlerin optimizasyonu sağlanmış, maliyetlerde azalmalar olmuş; üretimin hızlanmasıyla üretkenlik ve kârlılık gibi konularda da büyük artışlar meydana gelmiştir. Ancak bu teknolojik gelişmelerin denetim sürecine olumlu açıdan etkilerinin olduğu gibi olumsuz etkilerinin olduğu da aşikârdır. Bunlar içerisinde, teknolojiye uyum sağlayamayan personellerin olması ve bunun sürece olumsuz yansıması, teknolojinin çalışan davranışlarını gözlemleme konusundaki olumsuz boyutu, doğru analitik yöntemlerinin kullanılmamasıyla ortaya çıkan zaman kaybı, maliyet gibi olumsuzluklar yer almaktadır.

Geleneksel denetim yerini dijital denetime bırakmaya başlamış, denetimin dijitalleşmesinden büyük oranda fayda sağlamak isteyen denetçiler, yeni teknolojileri uygulayabilmek amacıyla dijital beceri ve yeteneklerini geliştirme çabasına girmiş; bu kapsamda eğitimlere yönelmişlerdir. Böylece denetim faaliyetini yerine getiren denetçilerin rollerinde bir kısım değişim ve gelişimler kaçınılmaz olmuş; sorumluklar artmıştır. Bu gelişmelere bağlı olarak, kaliteli denetim hizmeti sağlamak, denetimlerde ortaya çıkan hata ve hileleri minimum seviyeye indirmek, daha az zamanda daha çok iş yapmak, maliyetleri düşürmek gibi amaçlar denetimle ilgilenen tarafların birincil amaçları haline gelmiştir. Bu kapsamda denetim işini yapan kurum/kuruluşlar, bilgi teknolojilerini daha güvenilir, daha aktif, daha verimli hale getirmek ve daha kaliteli bir denetim süreci oluşturmak için teknolojik yatırımları hızlandırmaya başlamıştır. Bu çerçevede, çalışanlarını üst düzeyde eğitimlerle; müşterilerini ise çevrimiçi ve mobilde daha başarılı bir şekilde hazırlanmış olan uygulamalara geçirerek desteklemişlerdir. Bunun dışında denetim sürecine katkı sağlayacak bütün teknolojik uygulamaların kullanılmasına hız kazandırarak denetim sürecinin daha aktif bir şekilde işlerlik kazanmasını sağlamışlardır.

Ayrıca son zamanlarda yaşanan pandemi sürecinden dolayı uzaktan çalışma sistemine geçiş bütün alanları olduğu gibi denetim alanını da etkilemiştir. Denetim alanında yeterli teknolojik yeniliklerin olmaması ya da yetersiz olması uzaktan çalışma sürecini olumsuz etkilemiştir. Bütün alanlarda olduğu gibi denetim alanında da iletişim kalitesi dikkat edilmesi gereken hususlardandır. Dijital dönüşüme adaptasyon sorunu yaşayan çalışanların uzaktan çalışma sürecinde yaşadıkları iletişim sorunu çalışmalara olumsuz yansıyacaktır. Zayıf bir iletişim sadece çalışma performansını engellemeyecek aynı zamanda iş stresi oluşturarak bireylerin çalışma isteğini azaltacaktır (Wang vd., 2021, s. 34-35).

Bu kapsamda, sadece denetim işiyle ilgilenen kurum/kuruluşlar değil denetim alanında eğitim veren yükseköğretim çalışanı olan akademisyenler de denetimle ilgili bütün gelişmeleri yakından takip etmiş; araştırmaları ve çalışmalarıyla sürece katkı sağlamak istemişlerdir.

Bütün bu bilgiler ışığında, çalışmanın amacı denetim alanında yaşanan teknolojik gelişmelerin denetim sürecine olan etkilerinin ortaya çıkarılması olup; akademisyen görüşlerinin incelenmesidir. Çalışmanın ilk bölümünde denetim kavramına, denetimin dijitalleşmesi ve denetimde ortaya çıkan güncel yaklaşımlara değinilmiş; ikinci bölümde denetimin dijitalleşmesi kapsamında yapılan bazı akademik çalışmalar ve bulgularına yer verilmiştir. Çalışmanın son bölümünde ise, denetim alanında akademik çalışmaları olan akademisyenlerin denetimde güncel

yaklaşımlar bağlamında ortaya çıkan teknolojik uygulamaların denetim sürecine olan etkilerine ilişkin görüşlerine yer verilerek; değerlendirilmeler yapılmıştır.

2. KAVRAMSAL ÇERÇEVE

Denetim, kurumların işlem ve faaliyetlerinin daha önceden belirlenen amaçlara ve kurallara uygun bir şekilde yapılıp yapılmadığını tespit etmek amacıyla yapılan incelemeleri kapsayan bir süreçtir. Yönetimde yer alan önemli fonksiyonlardan biri olan denetim, organizasyonların başarısı için oldukça önemli bir işleve sahiptir (Bozkurt, 2013, s. 57). Bir diğer denetim tanımı ise, ekonomik bir birim ya da döneme ait olan bilgilerin belirlenmiş ölçütlere uygun olup olmadığını araştırmaktır (Gökbayrak, 2020, s.5). Denetim kavramıyla ilgili farklı kaynaklarda farklı anlamları taşıyan ve farklı isimlerle anılan ancak birbirlerinin yerine kullanılabilen terimler bulunmaktadır. Bunlardan bazıları; kontrol, teftiş, inceleme , izleme ve gözetim kavramlarıdır (Kebeli, 2020,s.7).

Yapılan bu tanımlara göre denetime ilişkin bazı özellikler ön plana çıkmaktadır. Bunlar;

- Denetim, sistematik bir süreç özelliği taşır.
- Denetim, iktisadi olaylar ve faaliyetlere ilişkin iddiaları kapsar.
- Denetim faaliyetinde, denetimin amacı doğrultusunda önceden belirlenmiş ölçütler kullanılmaktadır.
- Denetimde tarafsız kanıt toplama ve değerlendirme ön plandadır.
- Denetim faaliyetleri alanında uzman kişiler tarafından yapılmayı gerektirir.
- Denetim işlemleri sonunda rapor düzenleme gerekliliği vardır.
- Denetime ilişkin düzenlenen raporların ilgililere duyurulması gerekmektedir (Karacan, Uygun , 2012, s.24).

Manuel olarak oluşturulmuş verilerin ve iş akışlarının dijital ortamlara aktarılması olarak tanımlanan dijitalleşme kavramı, Endüstri 4.0 kavramı ile daha da önem kazanmıştır. Eldeki mevcut kaynakların bilgi teknolojilerinin ortaya çıkardığı fırsatları değerlendirerek optimal sonuçlara dönüştürmeyi amaçlayan dijitalleşme, son yıllarda bütün mesleki alanlarda varlığını hissettirmeye başlamıştır (Özen, Gürel, 2020, s.17). Ayrıca dijitalleşme, bilgilerin fiziksel bir bağlılık olmadan da sunulmasını ifade etmektedir (Erdoğan, 2020, s.3). Dijital dönüşüm, teknolojik gelişmelerin hayatın bütün alnlarında sunduğu fırsatlardan yararlanan köklü değişimlerdir (Aksoy & Gürol, 2021, s. 361). Yaşanan dijital dönüşümle beraber ortaya çıkan dijital faaliyetler, denetim mesleğinde de değişim ve dönüşümü gerekli kılmıştır. Elektronik olarak kaydedilen bir çok bilgi ve verinin geleneksel yöntemleri kullanarak denetlenmesinin mümkün olmadığı çağımızda,bilgi teknolojilerinin daha aktif kullanılması artık kaçınılmaz olmuştur. Verilerin toplanması, kaydedilmesi,depolanması, işlenmesi ve iletilmesi gibi süreçleri kapsayan bilgi teknolojileri bilgisayar ve telekomünikasyon ekipmanlarının kulanılmasını ifade etmektedir. Bu süreç artık denetim alanında da hızla ilerleme kaydetmektedir (Ghasemi vd., 2011, s.114).

Bilgilerin dijital ortama aktarılması ve yenilikçi yaklaşımlarla ilerlemesi, modern tekniklerle analiz edilmesi ve daha iyi hizmet verme işletmeler için oldukça önemlidir. Bunun yanısıra, işletmeler dijital döngüde daha aktif bir şekilde yer ve rol edinebilmek için, yeni nesil işletim modelleri oluşturmaktadır. Böylece, başarılı ve güncel bir dönüşüm yol haritası oluşturarak müşterilerine daha kaliteli hizmetler sunabilmektedirler (Celayir , Celayir, 2020, s.131) . Bütün bunların dışından dijitalleşmeyle beraber karamaşık bir hâl alan ve çeşitli dış etkenlere maruz kalan bir çok işletme ortaya çıkan riskleri erken tespit edebilmek için hem iç denetim hem de risk değerlenmdirmesi faaliyetlerine büyük ihtiyaç duymaktadır. Gelişen teknolojiler işletmelerin karşılaştığı zorluklar, fırsatları değerlendirmek için önem taşıyan iç denetim ve risk değerlendirmesi gibi konularda işletmelere bütük katkılar sağlyacaktır (Kahyaoğlu & Aksoy , 2021, s. 179).

Denetim firmaları, ortaya koydukları hedeflere ulaşabilmek için veri işlemeyi otomatikleştirmek ve insani müdahaleleri minimum düzeye indirmek için gelişen yeni teknolojileri yakından takip etmeye başlamış ve bilgi sistemlerinin giderek daha fazla entegre olması ve güvence altına alınmasını sağlamışlardır. Çünkü etkin bir bağımsız denetimden bahsedilmek, denetime ilişkin hedeflerin net olarak ortaya konmasını, şeffaflığı, hesap verilebilirliği, rekabet için yeniliğe ve gelişime açık bir denetim sisteminin varlığını gerektirmektedir (Bozkurt P. , 2013, s. 57). Günümüzde faaliyet gösteren birçok denetim firması, dijitalleşme konusunda önemli adımlar atmaya başlamış ve bu kapsamda iç süreçlerini giderek geliştirmektedirler. Bunun dışında, müşterilerine değer katmak maksadıyla denetim faaliyetlerindeki güncel yaklaşımlar kapsamında ortaya çıkan dijital yenilik ve araçlardan nasıl faydalanılabileceğini araştırmışlardır (Dengler, Matthes, 2018, s.307).

Denetim alanındaki teknolojik gelişmeler giderek daha hızlı bir şekilde ilerleme kaydetmektedir. Pek çok türde uygulanan yenilikçi denetim uygulaması bulunmaktadır. Fakat uygulanan bu yaklaşımlar ve teknolojik yeniliklerin denetimin verimliliğini arttırması konusunda farklı iyileştirme ve geliştirmelerin yapılmasını da kaçınılmaz kılmaktadır. Bu kapsamda mevcut yenilikçi denetimlere, yüksek katılımlı denetim mekanizması yeniliği eklenmeli ve denetimi daha da iyi seviyeye getirmeye odaklanılmalı ve gelişen bütün teknolojiler yüksek katılımlı denetime uygulanabilirlik açısından tespit edilmelidir. Böylece, çalışanlar ve diğer personeller de denetim sürecine entegre olacaktır. Bu durum hem denetim uygulamalarının verimliliğini hem de kalitesini arttıracak ilgili bütün taraflara yüksek düzeyde avantajlar sağlayacaktır (Öztürk, 2021, s.111). Yaşanan bu dijital evrimde ortaya çıkan yenilikçi ve güncel yaklaşımlar bağlamındaki teknolojik yeniliklerden bazıları veri analitiği ve büyük veri, blok zincir, akıllı sözleşmeler, yapay zekâ teknolojisi, bulut bilişim, siber güvenlik, dijital ikiz ve nesnelerin interneti gibi yeniliklerdir. Çağımızdaki en önemli gelişmelerden birisi de (Edge Computing) kenar bilişim, uç bilişim kavramıdır. 5G teknoloji ile birlikte birçok gelişmenin kapısını aralayacaktır.

Dört V'ye (volume, variety, velocity ve veracity) göre açıklanmış; yapılandırılmış ve yapılandırılmamış olan veri kümeleri olarak tanımlanan büyük veri kavramı, hacim (volume), çeşitlilik (variety), hız (velocity) ve gerçeklik (veracity) gibi unsurları içermektedir. Hacim kavramı, geleneksel olan araçların denetleme faaliyetinde yetersiz olduğu veri kümesini yansıtırken çeşitlilik nicel, metin tabanlı, karışık formların yanında resim, video gibi farklı formatları içeren veri formatlarıdır. Verilerin kullanılabilir düzeye gelme sıklığını ölçen ve giderek artış gösteren hız denetim de önem taşıyan bir diğer unsurdur. Denetimde verilerin kalitesinin güvenirliliği ve doğruluğu da gerçekliği yansıtmaktadır. Durmadan genişleyen ve büyüyen bir yapıya haiz olan denetim, gerçek zamanlı bilgiyle ve artan veri hızıyla karşı karşıyadır (Celayir, Celayir , 2020, s.135).

Büyük veriler, veri analizi yapan şirketler açısından oldukça önemlidir. Gelişmiş içgörü ve karar verme mekanizmalarıyla yenilikçi ve düşük maliyet içeren bilgi işleme şekillerini talep eden, yüksek hacimli ve farklılık arz eden bilgi varlıkları olarak tanımlanan büyük veriler, yenilikçi bir yaklaşımla analiz edilmeli ve işlenmelidir. Teknolojide ortaya çıkan bu gelişmeler, yenilikçi veri analiz araçlarının önemini ortaya koymuştur. Denetçiler, bu araçlar aracılığıyla daha büyük verileri analiz etmeye başlamışlardır. Böylece, büyük veri analizleri sayesinde bağlanabilirlik ve iç görüden faydalanarak, denetimle ilgilenen bütün paydaşlara bilgi aktarılması daha şeffaf olmakta ve denetlenen işletmelerin finansal raporlanmasına güven daha da artmaktadır (Celayir, Celayir , 2020, s.135). Veri analitiğini kullanan denetçiler, müşterilerine denetime ilişkin istatistikler, öneriler, kıyaslamalar sunabilmektedir. Riskler ve eğilimlerin daha güvenli biçimde tespit edilmesi sağlanarak müşterilere katma değer sağlanmaktadır. Daha başarılı risk değerlendirmeleri yapılarak denetimin verimliliği ve kalitesi arttırılmaktadır (Sultan, Ruhi, Lakhani , 2018, s.52).

Gerek ulusal gerekse uluslararası basında sıkça bahsedilen ve özel sektör, kamu kuruluşları tarafından büyük ilgi gören blok zincir, daha güçlü bir teknoloji olarak kabul edilmektedir. Dijital çağın en büyük yeniliklerinden biridir (Celayir, Celayir , 2020, s.136). Merkezi olmayan ve ortak bir kayıt veri sistemi olarak tanımlanan blok zincir, güvenilirlik, şeffaflık ve kesinlik ilkelerine bağlı kalarak; bilgilere şeffaf ulaşım sağlaması yönüyle denetimde ortaya çıkacak olan olumsuzlukların en aza indirilmesini amaçlamaktadır (Erturan, Ergin , 2018, s.815). Ortaya çıkan yeni blok zincir tabanlı teknikler sayesinde denetçilerin hem rollerinde hem de becerilerinde değişimler kaçınılmaz olacaktır. Yeterli denetim kanıtı elde etmek isteyen bir denetçi, hem genel muhasebe kayıtlarına hem de blockhain kayıtlarına dikkat etmek zorunda kalacaktır (Deloitte, 2017). Blok zincirin ortaya çıkardığı önemli kullanımlardan biri de akıllı sözleşmelerdir. Sözleşmelerin şartlarını tamamen otomatik bir şekilde yerine getiren bilgisayar programları olarak tanımlanan akıllı sözleşmeler, dijital protokoller tarafından uygulanan sözleşmelerdir (Özkul, Alkan, 2020, s.231). Muhasebe kayıtlarını tutmak amacıyla kriptografik paylaşımlı defterleri kullanan akıllı sözleşmeler, muhasebe işlemleri açısından hem zaman hem de maliyeti düşürme potansiyeline sahiptir. Gerçek zamanlı ve güvenilir raporlamanın sağlanması açısından da oldukça avantajlıdır (Gökten, Özdoğan , 2019, s. 435). Akıllı sözleşmelerin ödemelerde kullanılmasıyla hem verginin düşürülmesinde hem raporlamanın yapılmasında eş ve gerçek zamanlı işlemlerin yapılması sağlanacaktır. Akıllı sözleşmeler aracılığıyla, KDV oranları otomatik hesaplanacak ve toplam tutar içinde düşülerek direkt vergi makamına aktarılması sağlanacaktır. Ayrıca KDV iadeleri hızlı bir şekilde gerçekleştirilecektir. Böylece vergi kaçakçılığı, vergi kayıplarının önüne geçilmiş olunacak ve şeffaflık büyük ölçüde arttırılarak denetime destek sağlanacaktır (Özkul, Alkan, 2020, s.231).

Yapay zekâ ise, bilgisayar ve internet teknolojileri içerisinde yer alan bir diğer önemli teknolojidir. Akıllı asistanlar, sohbet robotları, öneri motorları gibi teknolojik yeniliklerle kendini ifade eden yapay zekâ teknolojisi son yıllarda hızla ilerleme kaydetmiştir (Celayir, Celayir, 2020, s.134). Yapay zekâ, muhasebe ve denetim

mesleğinin gelişmesine de büyük katkı sağlamıştır (Serçemeli, 2018, s.372). Denetim alanında faaliyet gösteren önemli denetim firmaları, çeşitli yapay zekâ ve yazılım araçları geliştirerek varlıklarını idame ettirme ve dijital dönüşüm sürecine kolayca adapte olmaya çalışmaktadırlar (Deloitte, 2017). Denetim sürecini iyileştirmek için denetim firmaları tarafından kullanılan yenilikçi ve güncel yaklaşımların en çok kullanılanı yapay zekâ ve big data'dır. Yapay zekâ yetenekleri , denetimde emek ve yoğun görevlerin otomasyonu şeklinde yer almıştır. Bu kapsamda denetim firmaları iş akışlarında yapay zekâ teknoljisine büyük önem vermiş; yapay zekâ teknolojisini firmalarına entegre ederek "*öğrenebilen"* bir uygulama geliştimişlerdir. Bu uygulama vasıtasıyla sözleşme türü belge analizlerinin daha sağlıklı ve etkin yapılabilmesini sağlamışladır (Celayir , Celayir , 2020, s.134).

Dijitalleşme sürecinde internet ve mobil teknolojilerin giderek yaygınlaşması sonucu, bulut bilişim de bilgi teknolojilerinde ön plana çıkan yenilikçi yaklaşımlardan biri olmuştur. İşletmelerin iş yapmalarını önemli ölçüde etkileyen bulut bilişim, işletmeleri iki yönlü etkilemektedir. Bulut bilişim teknolojisini kullanan şirketlerin denetimi, bilişim sistemlerinin de denetimini gerektirmektedir. Kullanılan modele uygun olarak riskler tespit edilmeli, buna yönelik kontroller değişmeli ve uygun denetim yaklaşımı tercih edilmelidir. İkinci durum ise, işletmeler denetim uygulamalarını bulut ortama taşımalıdırlar. Denetçiler, internet erişiminin sağlandığı her yerde bulut bilişim teknolojilerini kullanarak etkin ve verimli kaynak erişimi sağlayabilirler. Böylelikle, internet ulaşımı sağlanan her yerden denetim faaliyetleri kolayca yapılmakta, denetimde verimlilik ve kalite artmakta, eş zamanlı denetim yapılabilmektedir. Bu durum rekabette kolayca üstünlük sağlama açısından avantajlı olmaktadır (Ciğer, Kınay, 2018, s.632).

Bilgisayarları, ağları, programları ve verileri korumak adına tasarlanmış olan teknoloji ve süreçler bütünü olarak tanımlanan siber güvenlik, kurumların bilgilerine güvenli bir şekilde erişilmesine olanak sağlayan ortak etkinlik ve kaynakları kapsamaktadır (Celayir, Celayir , 2020, s.137). Siber güvenlik, denetim faaliyetini yürüten bir çok firma açısından önemli riskler barındırmaktadır. Bir denetim firmasına ait olan siber güvenlik altyapısının yetersiz olması halinde ciddi bir saldırı ile karşı karşıya gelmesi, müşterileri tarafından hoş karşılanmamaktadır. Bu durum işletmeye geri dönülmez zararlar verebilir. Bu sebeple, denetim firmaları bu tür siber tehditleri ön görüp risk değerlendirmesini ve risk yönetim sürecini bu yönde şekillendirmelidirler (KMPG, 2017).

Dijital ikiz kavramı, gerçek dünya koşullarını analiz eden, simüle eden, değişikliklere yanıt vererek işlemleri gerçekleştiren fiziksel bir nesnenin ya da sistemin dinamik yazılım modeli olarak tanımlanmaktadır. İşletmeler tarafından dijital ikiz teknolojisinin kullanılması, maliyeti düşürme noktasında ve işlemlerin gerçekleştirilmesinde optimizasyon sağlanması açısından tercih edilmektedir. Dijital ikiz teknoljisiyle oluşturulan ve kullanılan modeller, sorunların ortaya çıkmadan önce tespit edilmesi, üretimin kârlı bir şekilde arrtırılması ve planması, verimiliğin arttırılması gibi konularda büyük fayda sağlamaktadır. Bunların dışında dijital ikiz, bilgilerin sürekli izlenmesi, bilgi kalitesi ve geçerliliğini inceleme konusunda denetçilere büyük avantajlar sunacak; denetim sırasında ortaya çıkan hata ve hilerin daha kolay belirlenerek analiz edilmesini kolaylaştırcaktır. Dijital ikizle elde edilen veri analizleriyle desteklenen denetim süreciyle finansal tabloların ötesine geçilecek, karmaşık yapıya sahip organizasyonların incelenmesi, anlaşılması, operasyonel süreçlerdeki bulgular hakkında karar verecek merciilere kaliteli bilgi üretme imkanı sağlanacaktır (Erturan, Ergin , 2018, s.815-816). Nesnelerin interneti, işlerin planlanması, kaynakların verimli kullanılması, bilgilerin gerçek zamanlı olarak alınmasını sağlayarak, işletme süreçlerinin iyileştirilmesi, maliyetlerin azaltılması ve risklerin daha etkin yönetilmesine katkı sunmakta; işlemlerin daha doğru bir şekilde denetlenmesinde denetçilere yol göstermektedir (Murphy, 2015). Son zamanlarda denetim alanında ortaya çıkan bir diğer önemli güncel yaklaşım ve denetim türü olan iç denetimdir. İç denetim, kamu kesimi yönetişimin temel unsurları içerisinde yer alan ve denetim alanında önemli yeri olan bir kavramdır. İç denetim "*genel anlamda kamu yönetimi sistemi içinde yer alan herhangi bir kurum veya kuruluşun, hiyerarşik olarak veya oluşturduğu denetim organları aracılığıyla kendi birimleri üzerinde denetimi*" olarak tanımlanmaktadır (Kebeli, 2020, s.7). Etkili bir iç denetimin faaliyetinin varlığı kamusal yönetişimin güçlenmesine katkı sağlamakta, kamuda ortaya çıkabilecek yolsuzluk risklerini minimize etmekte ve kamu yöneticilerinin daha adil davranmasında, güvenilir olmasında büyük rol oynamaktadır. Bu nedenle kurumsal yönetim açısından oldukça büyük öneme sahip olan iç denetim faaliyetleri, resmi bir prosedüre bağlı olmalı; bu faaliyeti yürüten iç denetçilerin görev ve yetki açık bir şekilde yasal zemine oturtulmalıdır (Aytar, 2022, s.17). Ayrıca iç denetçilerin teknolojik yenilikleri yakından takip ederek denetim faaliyetlerinde uygulamaları, kendilerini sürekli geliştirmeleri ve bu noktada desteklenmeleri denetimin başarılı bir şekilde yürütülmesinde oldukça önemli bir yere sahiptir.

Edge Computing, son yıllarda büyük gelişme göstererek tasarlanmış bir BT teknolojisidir. Ayrıca IoT'nin gelişimine bağlı olan bilgi işlem alt yapısıdır. Mümkün olduğunca yakın uygulamalar sunan, noktaları birbirine yaklaştırdığından kullanıcı ihtiyaçlarına cevap vererek; gecikme sorunları da minimize eden bir sistemdir (Kars,

2021, s.14). 5G teknolojisiyle gelişim gösteren bu yenilikler, ağlara kolay erişim sağlama açısından köklü değişiklikler önermektedir. Verilerin hesaplanarak, depolanması, toplanması ve cihazlara yakınlaştırılması gibi avantajlar sunmaktadır. 5G ağlarının gelişmesiyle birlikte bir çok alanda gelişimde yaşanmaktadır. Bunlardan bazıları; endüstriyel otomasyon, kendi kendini süren arabalar, akıllı şehirler ve AR gibi teknolojilerdir (Siriwardhana vd., 2021, s. 1170).

Sonuç olarak yenilikçi yaklaşımlar çerçevesinde ortaya çıkan teknolojik gelişmeler ve dijitalleşme süreci, denetçilerin denetim süreçlerini, denetim kontrollerini ve uygulanan prosedürleri değiştirerek yeni denetim türleri, ortamları ve uygulamaları oluşturacaktır. Böylece denetim faaliyetleri ve denetim kalitesine değer katılacak ve dijitalleşme uyum süreçleri daha da hız kazanacaktır.

3. LİTERATÜR

Son yıllarda dijital dönüşüm önem kazanan ve sürekli gelişim gösteren bir durum haline gelmiştir. Bu yüzden birçok meslek gurubu dijital dönüşümde yaşanan teknolojik gelişmelerden faydalanmayı tercih etmiştir. Bu durum, araştırmacıların da dijital dönüşüm sürecine ve alanlarıyla alakalı olan güncel gelişmelere olan ilgisini arttırmış ve bu kapsamda yapılan ulusal/uluslararası akademik çalışmaların sayısı artmıştır. Yapılan çalışmalar incelendiğinde denetim alanında faaliyet gösteren denetçi, denetim firmaları, denetim alanında araştırma yapan akademisyen camiası vb. meslek mensuplarının dijital dönüşümü işlerin yürütülmesinde temel alması ve denetim alanındaki güncel yaklaşımlar ve teknolojik ilerlemelere bakış açıları gibi birçok konu araştırılmıştır. Buna ilişkin olarak literatürde yer alan akademik çalışmaların bazılarına aşağıda yer verilmiştir.

Acar vd. (2016), dijital ortamda sürekli denetime ilişkin inceleme yapmayı hedefledikleri bu çalışmalarında, sürekli denetim faaliyetine ilişkin verilerin dijital ortamlara kaydedilmesi, raporlanması ve analiz edilmesinin denetime olumlu etkilerinin olduğunu açıklayarak; dijitalleşen dünyada sürekli denetim sürecine, gereksinimlerine, usul ve esaslarına değinmişlerdir.

Özdemir ve Sağıroğlu (2017), bu çalışmalarında geleceğin denetiminin bugünün denetiminden çok daha farklı olacağını savunmuşlardır. Denetçilerin değişime açık olması gerektiği ifade edilmiş büyük veri ve analitiği incelenmiştir. .Konuya ilişkin temel unsurların gözden geçirilerek, büyük veri analitiğinden denetim faaliyetlerinde nasıl yararlanılacağına ve denetime nasıl entegre edileceğine ilişkin bir takım soruların cevaplanması amaçlanmıştır. Çalışma sonunda, denetimde ön plana çıkan büyük veri analitiği ile hızlı, verimli, kapsamlı ve daha fazla değer katan denetim faaliyetlerinin gerçekleştirilebileceğini öne sürmüşlerdir.
Karaduman (2017) çalışmasında, muhasebe denetiminde yapay zekâ ve XBRL kullanımının denetim süreci üzerindeki etkilerini ortaya koymayı hedeflemiştir. Çalışma sonucunda, denetime tabi işletmelerin yapay zekâ teknolojilerini muhasebe denetiminde kullanmalarıyla, standartlaşmanın sağlanacağı, denetime olan güvenin artacağı, şeffaf ve istikrarlı bir ekonomiye zemin hazırlanacağı gibi sonuçlar elde etmiştir.

Serçemeli (2018), çalışmasında hem muhasebe hem denetim mesleklerinde yapay zekâ teknolojilerinden etkilenmiş olduklarını ve bu durumun kaçınılmaz bir hal aldığını ifade etmiştir. İşletmelerin gerek muhasebe gerekse denetim alanındaki bu değişim sürecine ayak uydurulabilmeleri için ekonomik, teknik ve personel gibi konulara ilişkin yatırım yapmaları gerektiğini savunmuştur.

Erturan ve Engin (2018), denetim dijitalleşmesinin bir gereklilik olduğunu savundukları bu çalışmalarında, işletmelere ait olan finansal ve finansal olmayan verilerin eş zamanlı olarak dijital ortama aktarılmasının denetçiye verilere istenilen yerde ulaşma fırsatı sunması, hızlı ve kaliteli bilgi akışının sağlanması, hata ve hilelerin daha kolay tespit edilmesiyle yönetim nezdinde güven teşkil edilmesi gibi açılardan avantaj sağladığı sonucunu elde etmişlerdir.

Taş ve Mert (2019), denetimde yapay zekâ teknolojisine yer verdikleri çalışmada, yaşanan teknolojik gelişmelerin denetime olan etkilerini incelemeye çalışarak; denetimde kullanılan yapay zekâ örneklerine değinmişlerdir. Çalışma sonucunda, yapay zekânın işletmelerde verimli bir şekilde kullanılabilmesi için ERP sisteminin geliştirilmesinin bir zorunluluk olduğu ve bağımsız denetim yapan firmaların yapay zekâ tasarlamalarının muhtemel zorluklarının olduğu sonucuna ulaşmışlardır.

Zhang (2019) yılındaki çalışmasında, denetim süreçlerinde akıllı süreç otomasyonunun kullanılmasının bir takım faydaları olduğunu savunmuştur. Bu faydaların denetim faaliyetlerinin etkin ve verimliliğine katkı sağlayacağı yönünde görüş bildirmiştir.

Celayir ve Celayir (2020), dijitalleşmenin denetim mesleğine olan etkilerini incelemeyi amaçlamışlardır. Bu kapsamda yaptıkları çalışmalarında, teknolojik gelişmelerin ve dijitalleşmenin denetim süreçlerine, denetim uygulamalarına ve mesleğine bir takım etkilerinin olduğunu öne sürmüşlerdir.

Manita vd. (2020), dijital gelişmelerin denetim ve yönetişim faaliyetleri üzerindeki etkilerini incelemeyi amaçladıkları çalışmalarında, Fransa'da yer alan ve en büyük beş denetim firmasının denetçileriyle görüşerek dijitalleşmenin denetim firmalarını ve denetim rolünü nasıl etkilediğini ortaya çıkarmak istemişlerdir. Araştırma sonucunda, dijitalleşmeyle birlikte denetçinin müşterilerinin verilerini analiz ederek kaliteyi arttıracağı, yeni bir denetçi profilinin oluşacağı gibi etkilerinin olduğu sonucuna varmışlardır. (Manita, Ellomal , Baudier, & Hikkerova, 2020).

Yel ve Atasoy (2021), çalışmalarında dijital veri ve yöntemleri temel alarak gerçekleştirilen dijital denetim sürecinin güvenliğe ilişkin etkilerini incelemek amacıyla KGK kayıtlı olan ve aktif çalışan bağımsız denetçilere bir anket çalışması uygulamışlardır. Bu çalışmada, denetçilerin dijital sürece uyumlarını, dijital süreçten bekledikleri faydayı, dijital denetimin kalitesini ve dijital veri güvenliğine uyum sağlama düzeylerini araştırmışlardır.

4. DENETİMDE TEKNOLOJİK GELİŞMELERİN DENETİM SÜRECİNE OLAN ETKİLERİNİN AKADEMİSYEN GÖRÜŞLERİYLE İNCELENMESİNE YÖNELİK ARAŞTIRMA

Bu bölümde araştırmaya ilişkin model, çalışma grubu, verilerin toplanması, verilerin analizleri ve araştırmanın güvenilirliği, geçerliliği ile ilgili bilgilere yer verilmektedir. Araştırmada kullanılan araştırma formu, Bitlis Eren Üniversitesi Etik İlkeleri ve Etik Kurulu tarafından 15.02.2022 tarihinde 22/02-4 sayılı ve E.1769 evrak kayıt kararıyla uygun görülmüştür. (Sayı: E-84771431-050.03-40650)

4.1.Araştırma Modeli

Nitel araştırma çerçevesinde oluşturulmuş olan bu araştırma, kuram oluşturmaya yönelen bir anlayışla sosyal olguları bulundukları çevre içerisinde araştırmayı ve anlamayı ön planda tutan bir araştırma türüdür. Nitel araştırmaların herkes tarafından kabul gören bir tanımını yapmak zor olsa da "*görüşme, gözlem, odak grup görüşmesi, doküman/belge ve resim analizi gibi nitel yöntemlerin kullanıldığı, olayların doğal ortamlarda gerçekçi ve bütüncül bir şekilde oluşmasına yönelik sürecin izlendiği araştırma*" olarak tanımlanmaktadır (Yıldırım, Şimşek, 2011). Nitel veri desenlerinden olan betimsel desenle yapılmış olan araştırmada akademisyenlerin denetimde güncel yaklaşımların denetim sürecine olan etkilerine ilişkin görüşlerinin özgün forma bağlı kalarak doğrudan alıntılarla betimlenmesi ve sunulması amaçlanmıştır. Ayrıca gönüllülük esası ön planda tutulmuş ve katılım sağlayanlarla yüz yüze görüşme formu tekniği kullanılması istenmiştir. Ancak mesafe, barınma, pandemi süreci gibi durumların etkisinden kaynaklı katılım sağlayanlarla mail yoluyla bağlantı kurulmuş ve gerekli yönlendirmeler bu şekilde yapılmıştır.

4.2. Çalışma Grubu

Araştırmanın çalışma grubunu denetim alanında akademik çalışmaları bulunan hem özel hem de devlet üniversitelerinde akademisyen statüsünde çalışanlar oluşturmaktadır. Araştırmanın amacına ulaşabilmesi için çalışma grubu temel alınarak ölçüt örneklem yöntemi kullanılmıştır. Ölçüt örneklem, yapılan bir araştırmada belirli niteliklere sahip bireylerin, olayların ya da nesnelerin yer verildiği örneklem türüdür(Büyüköztürk, Çakmak, Akgün, Kadeniz, Demirel, 2014). Nitel araştırmalarda yer verilen örneklem sayısı 1 'de olabilir 12 'de olabilir (Potton, 1990). Araştırmaya katılım sağlayan 14 akademisyenle gerekli görüşmeler yapılmış ve çalışmaya gönüllülük esasına dayalı olarak katkı sağlamaları gerçekleştirilmiştir.

4.3. Araştırmanın Amacı, Veri Toplanması Ve Araştırma Soruları

Çalışmanın amacı, denetimde ortaya çıkan güncel yaklaşımlar ve teknolojik yeniliklerin denetim sürecine olan olumlu ya da olumsuz etkilerinin ortaya çıkarılmasıdır. Bu kapsamda denetim alanına ilişkin akademik çalışmaları bulunan akademisyen görüşlerinin incelenmesi hedeflenmiştir. Bu amaç doğrultusunda araştırma soruları yapılan literatür taraması sonucu oluşturulmuş; görüşme formu tekniği yoluyla araştırmanın amacına uygun 7 adet soru araştırmaya gönüllü olarak katılan akademisyenlere yöneltilmiştir. Araştırmanın soruları aşağıdaki gibidir:

1. Denetim faaliyetlerinde teknolojiden yeterli düzeyde yararlanıldığını düşünüyor musunuz?

2. Denetim alanında kullanılan güncel yaklaşım ve teknolojilerin üstünlükleri ve sakıncalarından bahseder misiniz?
3. Denetim faaliyetlerinde uygulanan teknolojilerin (yapay zekâ, entegre raporlama, blok zincir, akıllı sözleşmeler vb.) aksaklık, hata ve hile konularında nasıl bir etki oluşturduğunu düşünüyorsunuz? Bu konuda neler söylersiniz?
4. Denetim faaliyetlerinde uygulanan teknolojilerin (yapay zekâ, entegre raporlama, blok zincir, akıllı sözleşmeler vb.) denetim sürecine ve kalitesine etkisi var mıdır? Bu konuda neler söylersiniz?
5. Denetim işini yürüten kişi/kişiler/kurumların kullanılan teknolojik gelişmelere uyum sağlayabildiklerini düşünüyor musunuz? (Uyum ile ilgili önerileriniz nelerdir?)
6. Denetimler yapılırken uygulanan yaklaşımların, teknolojik yeniliklerin denetimin verimliliğine katkısı olduğunu düşünüyor musunuz? Bu konuda neler söylersiniz?
7. Denetim faaliyetlerinde çağdaş yaklaşım ve teknoloji kullanımlarının denetçilerin yerini alabileceği diğer bir ifadeyle istihdamı azaltacağı yönündeki düşüncelere katılıyor musunuz? Bu bağlamda neler söylersiniz?

4.4. Araştırma Verilerinin Analizi

Akademisyenlerden elde edilen veriler elektronik ortama aktarılarak kavramsallaştırılmış ve bu veriler daha sonra ortaya çıkan kavramlara göre düzenlenmiştir. Düzenlenen verileri açıklayan temaların belirlenmesini sağlamak amacıyla içerik analizi yöntemine başvurulmuştur (Yıldırım, Şimşek, 2013. Araştırmadan elde edilen veriler içerik analiziyle ve doğrudan alıntılarla desteklenerek öneriler getirilmiştir.

4.5. Araştırmanın Geçerliliği ve Güvenirliliği

Araştırma sonucunda elde edilen verilerin tümü ham haliyle saklanmış ve bu şekilde araştırmanın dış güvenirliğinin arttırılması hedeflenmiştir. Görüşme formundaki sorular açık ve anlaşılır bir şekilde ifade edilmiş, çalışmanın amacı doğrultusunda ayrıntılı olarak toplanmaya çalışılmıştır. Böylece araştırmanın iç güvenirliğinin sağlanması hedeflenmiştir (Yıldırım, Şimşek, 2013). Araştırmanın bütün verileri üzerinde ayrı ayrı yapılan kodlamalar birbirleri ile karşılaştırılarak kodlamalar arasındaki tutarlılık incelenmiş, elde edilen kodların birbirine benzer ve uyumlu olduğu sonucuna varılmıştır. Araştırmada doğrudan alıntılar yapılarak akademisyenlerin görüşlerine yer verilmesi ve araştırma bulgularının kendi içinde tutarlılık göstermiş olması araştırmanın geçerliğinin sağlandığını göstermiştir.

4.6. Araştırma Bulguları ve Değerlendirme

Çalışmanın bu bölümünde araştırma sonucunda elde edilen bulgulara ve değerlendirmelere yer verilmiştir. Araştırmada elde edilen verilerin analizleri yapılırken katılımcılara birer kod verilmiş; her katılımcı gizlilik ilkesi gereğince "AK1, AK2,…, AK14" şeklinde kodlanmıştır.

4.6.1. Denetim Faaliyetlerinde Teknolojiden Yeterli Düzeyde Yararlanıldığına İlişkin Bulgular ve Görüşler

Son yıllarda denetim faaliyetlerinin giderek gelişim göstermesiyle teknolojiye ihtiyaç artmış ve birçok denetim firması teknolojiden üst düzeyde yararlanmaya özen göstermiştir. Bu çalışma kapsamında "denetimde katılımcıların teknolojiden yeterli düzeyde yararlanılıp/yararlanılmadığına ilişkin görüşlerini" paylaşmaları istenmiştir. Yapılan görüşme sonucunda 14 katılımcıdan 9'u yararlanıldığı; 5'i ise yararlanılmadığı yönünde görüş bildirmiştir. Katılımcıların konuya ilişkin görüşlerinden bazıları aşağıdaki gibidir:

Katılımcı AK1: "*Ülkemiz özelinde düşündüğümüzde denetim faaliyetlerinin yürütülmesinde bilgi teknolojisi ürünlerinden yeterince faydalanılmadığı söylenilebilir ancak kısmen de olsa teknolojik ürünlerden fayda sağlanmaktadır. örneğin kamu da iç denetim faaliyetlerinin yürütülmesinde "içden" adlı yazılım programının sağlık sektöründe ise dijital denetimin dönüşümü için hazırlanan deniz programının kullanılması atılan adımlar arasında gösterilebilir. ancak bunların çok sınırlı olduğu görülmektedir özellikle Pandemi döneminde denetim faaliyetlerinin uzaktan yürütülmesi gerekliliği doğmuştur bu alanda yapılan çalışmalara bakıldığında uzaktan denetim faaliyetlerinin yürütülmesinde tamamen denetim faaliyetlerine odaklı bilgi teknolojisi ürünlerinin kullanılmadığı görülmektedir dolayısıyla denetim faaliyetlerinin yürütülmesinde teknolojiden yeterli düzeyde yararlanıldığı söylenemez*."

Katılımcı AK2: "*Denetim faaliyetlerinde teknolojinin önemi büyük ancak denetim faaliyetlerinde teknolojiden tam olarak yararlanılmadığı söylenebilir. Teknolojinin belirli bir maliyetinin olması nedeniyle bazı kurumsal*

birimlerin dışında hala eski tekniklerin uygulanması durumu olabilmekte. Bilgisayar destekli denetim araçlarının daha yaygın kullanılması ile teknolojiden yeterli düzeyde yararlanılabilir."

Katılımcı AK8: "*Bankacılık sektörü başta olmak üzere kurumsal firmaların denetimde teknoloji odaklı uygulamaları faaliyetlerine entegre ettikleri izlenmektedir. Bunun yanında KOBİ niteliğindeki şirketlerin faaliyet süreçlerinde teknolojiye yönelim daha yavaş seyretmekte olup söz konusu firmaların denetim metodolojilerinin teknoloji tabanlı olmaktan bir hayli uzak olduğu söylenebilir."*

Katılımcı AK11: "*Özellikle dört büyükler ve uluslararası ortaklı işletmelerde teknolojik yeniliklerden yeterli düzeyde yararlanıldığını düşünüyorum*."

Katılımcı AK14: " *Denetim faaliyetlerinde gerekli düzeyde teknolojik yeniliklerden yararlanıldığını düşünüyorum. Kullanılan yapay zekâ teknolojisi, dijital ikiz, blok zincir teknolojilerinin son zamanlarda denetim faaliyeti yürüten firmalar ile, bankacılık sektöründe kullanıldığı görülmektedir. Bu açıdan teknolojinin yeterli düzeyde olduğu kanısındayım ancak daha da yüksek düzeye çıkarılabilir".*

4.6.2. Denetim Alanında Kullanılan Güncel Yaklaşım ve Teknolojilerin Üstünlükler ve Sakıncaların Tespitine İlişkin Bulgular ve Görüşler

Araştırmaya katılım sağlayan akademisyenlerin çoğunluğu kullanılan güncel yaklaşım ve teknolojilerin hata ve hile konusunda üstünlükleri olduğu; güvenlik gibi konularda ise sakıncaları olduğu yönünde görüş birliği sağlamışlardır. Bu çerçevede akademisyenlerin bu konuyla ilgili görüşlerinden bazılarına aşağıda yer verilmiştir:

Katılımcı AK7: "*Denetim sürecinin teknolojiden yararlanılarak yapılması durumunda olası hataların önleneceğini ancak siber saldırılara uğrama olasılığının bulunması ihtimali denetim sürecinde aksamaların yaşanmasına yol açabileceğini düşünüyorum ."*

Katılımcı AK9: "*Üstünlüklerinin zaman ve maliyet tasarrufu; sakıncalarının ise güvenlik sorunları şeklinde olduğunu düşünüyorum."*

Katılımcı AK10: *"Zamandan tasarruf, yönetici ve personelle yüz yüze gelmemek, daha rahat bir şekilde denetleme imkânı sağlaması, denetleme sırasında yaşanacak gerginlik ve uyuşmazlıkların yaşanmaması olumlu yönleri, teknolojinin insan yerini alması, istihdamın azalması, denetleyici ile müşteri işletme arasında muhabbetin azalması olumsuz etkilerdir."*

Katılımcı AK13: " *Zaman bakımından denetçilere tasarruf, maliyetlerde düşüşe katkı sağlaması, kayıtlarda oluşabilecek hata ve hilelerin daha kolay tespiti gibi üstünlüklerinin olduğu kanısındayım. Bütün alanlarda olduğu gibi denetim alanında da teknolojinin güvenlik sorunu, çalışanlar arasında, denetlenen-denetleyen firmalar arasında iletişim eksikliği gibi sorunlara yol açması nedeniyle sakıncalı olduğu düşüncesindeyim."*

4.6.3. Denetim Faaliyetlerinde Uygulanan Teknolojilerin (yapay zekâ, entegre raporlama, blok zincir, akıllı sözleşmeler vb.) Aksaklık, Hata ve Hile Konularındaki Etkilerinin Tespitine Yönelik Bulgular ve Görüşler

Katılımcıların denetim sırasında uygulanan yaklaşım ve teknolojik gelişmelerin aksaklık, hata ve hile konusuna nasıl bir etkisi olacağı yönündeki görüşlerini öğrenmek maksadıyla yöneltilen soruya verdikleri yanıtlara bakıldığında tümünün olumlu etkisi olduğu yönünde görüş bildirdiği sonucu ortaya çıkmış; verilen yanıtların bazılarına aşağıda yer verilmiştir:

Katılımcı AK5: "*Tabii parantez içinde ifade edilen her yaklaşımın ayrı ayrı ele alınması gerekir. Genel olarak bu teknolojilerin hata ya da hileleri tespit etmede insandan birçok konuda üstünlükleri olacaktır. Buna karşın denetimin bir de insani yani psikolojik yönü de vardır. Bazı durumlarda teknik anlamda her şey yolunda gözükür ama birtakım psikolojik unsurlar yardımıyla ilgili hata ya da hile tespit edilebilir."*

Katılımcı AK1: "*Denetim alanında kullanılan yapay zekâ, blokzincir, akıllı sözleşmeler gibi uygulamalar sayesinde denetimde hata ve hilenin önemli ölçüde azalabileceğini hatta özellikle blokzincir teknolojisi sayesinde makul düzeyde verilen güvencenin mutlak güvence şekline dönüşebileceğini bu gelişmelerin de gerek denetimin tanımında gerekse denetim süreçlerinde önemli değişikliklere yol açabileceğini düşünüyorum."*

Katılımcı AK3: "*Özellikle yapay zekâ uygulamaları ile anomalilerin rahatlıkla tespit edilmesi normalden sapan işlem örüntüleri ve davranış kalıpları hakkında kolayca ve hızlıca bilgi sahibi olunması mümkün hale gelmiştir.*

Doğası gereği hileler, bir nevi anomaliler olarak değerlendirildiğinde başta hile tespit ve önleme mekanizmalarının etkin ve sağlıklı bir yapıya kavuşturulması açısından yapay zekânın kritik bir işlev üstlendiği söylenebilir."

Katılımcı AK6: "*Aksaklık, hata ve hilelerin bu sayede daha kolay tespit edilebildiğini söyleyebiliriz."*

4.6.4. Denetim Faaliyetlerinde Uygulanan Teknolojilerin (yapay zekâ, entegre raporlama, blok zincir, akıllı sözleşmeler vb.) Denetim Sürecine ve Kalitesine Etkisini Belirlemeye İlişkin Bulgular ve Görüşler

Yapılan araştırmada denetim alanındaki güncel yaklaşımların ve teknolojik yeniliklerin denetim sürecine ve kalitesine etkisinin olup/olmadığının tespit edilmesi hedeflenmiştir. Bu kapsamda oluşturulan ve katılımcılara yöneltilen soruya verilen yanıtlar değerlendirildiğinde, denetim alanındaki güncel yaklaşımların ve teknolojik yeniliklerin denetim kalitesini arttıracağı ve sürece olumlu katkı sağlayacağı yönünde görüşlerin olduğu ortaya çıkmıştır. Ancak bu durumun iletişim noktasında zaman zaman sıkıntılar oluşturabileceği yönünde görüş bildirenler de olmuştur. Görüşlerden bazıları şöyledir:

Katılımcı AK4**: "***Denetim faaliyetlerinde daha şeffaf raporlamaların oluşması, denetimde güvencenin sağlanması gibi açılardan olumlu etkisi kaliteye de olumlu yansıyacaktır. Elbette kaliteli bir şekilde ortaya çıkan denetim faaliyetinde denetim süreci kısalacak ve zamandan tasarruf sağlanacaktır. Bu nedenle bu uygulamaların hem denetim kalitesine hem de sürecine yükse düzeyde olumlu etkisinin olduğu düşüncesindeyim."*

Katılımcı AK8: *"Uygulanan yaklaşımları geçmişle kıyasladığımızda denetim faaliyetleri daha çeşitli ve sayıca daha fazladır. Uygulanan yaklaşımların daha çeşitli ve fazla olması karmaşıklığı arttıracaktır. Denetimlerin daha kısa sürede olması ile ister istemez bu yaklaşımlar ihtiyaç haline gelmiş ve kalite açısından değerlendirildiğinde kaliteyi arttırıcı etkisi söz konusudur. Uygulanan yaklaşımlarla veriler daha kolay elde edilebilir, risk değerlendirmesi daha doğru yapılabilir, denetim planı daha kolay hazırlanabilir, hesaplamalar ve analizler daha kısa sürede doğru bir şekilde yapılabilir, erişim kolaylığı sağlanabilir, denetimde bazı kontrol uygulamaları ile denetimin güvence seviyesi arttırılabilir, gerçeğe uygun veriler ve analiz ile kaliteli denetim görüşü sağlanabilir."*

Katılımcı AK10: "*Etkisi olacaktır, ancak hoşgörü, idare etme, olumlu yönlerine bakma durumları geri plana itilir."*

Katılımcı AK12: "*Bu alanda çalışma yapmış biri olarak şunları söyleyebilirim: uygulanan teknolojik gelişmelerin denetim sürecine ve kalitesine olumlu etkisi olacağını düşünüyorum. Özellikle maliyeti düşürme açısından sürece; şeffaflık, anlaşılabilirlik ve güvence açısından ise kaliteye olumlu etkileri vardır. Ancak teknolojilerin kullanılmasıyla denetlenen- denetleyen firma çalışanları arasında zaman zaman iletişim konusunda sıkıntılar (iletişim eksikliği, yanlış ya tam anlaşılmama gibi) ortaya çıkabilir bu durumda hem denetimin işleyişine haliyle kalitesi ve sürecine de olumsuz etki edebilir. Bu nedenle dikkat edilmesi gereken önemli bir husustur".*

4.6.5. Denetim İşini Yürüten Kişi/Kişiler/Kurumların Kullanılan Teknolojik Gelişmelere Uyum Sağlamalarına İlişkin Bulgular ve Görüşler

Denetim faaliyeti kadar denetim yapan kişilerin de denetimle ilgili yeterli donanıma sahip olması oldukça önemlidir. Denetimi yapan kişilerin yaşanan teknolojik gelişmeleri yakından takip ederek; teknolojik gelişmelerin denetimde uygulanabilirliğini araştırmaları ve kendilerini bu yeniliklere göre sürekli geliştirmeleri kaçınılmaz bir gerçekliktir. Bu nedenle katılımcılara " *Denetim işini yürüten kişi/kişiler/kurumların kullanılan teknolojik gelişmelere uyum sağlayabildiklerini düşünüyor musunuz? (Uyum ile ilgili önerileriniz nelerdir?)"* sorusu yöneltilmiş bu konuyla ilgili birbirinden farklı görüşlerin ortaya çıktığı görülmüştür. Bazı katılımcılara ait görüşlere aşağıda yer verilmiştir.

Katılımcı AK1: "*Özellikle kamu sektöründe çalışan denetçilerin denetim alanında yaşanan teknolojik gelişmelere yeterince uyum sağladıkları söylenemez. Bu konuda özel sektörün daha iyi olduğunu düşünüyorum bu noktada gerekli uyumun sağlanabilmesi için bilgi teknolojileri denetimi konusunda gerekli eğitimlerin meslek kuruluşları tarafından verilmesi denetçilerin bu alanda kabul gören uluslararası mesleki sertifikaları alması gerekir."*

Katılımcı AK5: "*Tam olarak uyum sağladıklarını düşünmüyorum. Uyum için öncelikle kurumların ekonomik olarak yapacakları yatırım ile elde edecekleri verimlilik konusunda ikna edilmesi gerekir."*

Katılımcı AK6: "*Genç nesilde uyum daha kolayken eski nesilde uyum daha zor olmaktadır. Uyumun sağlanması için eski neslin öncelikle olayı kabullenmesi ve gerekli eğitimleri alması gerekmektedir."*

Katılımcı AK11: "*Bağımsız denetim sürekli gelişen ve değişen mevzuata sahip bir faaliyet içinde olduğu için mensuplarının sürekli öğrenme tarzına yatkınlığı söz konusudur. Bu yönüyle onların yeni teknolojilere entegrasyon bakımından avantajlı bir kitle olduklarını düşünmekteyim.*"

4.6.6. Denetimler Yapılırken Uygulanan Yaklaşımların, Teknolojik Yeniliklerin Denetimin Verimliliğine Katkısının Değerlendirilmesine İlişkin Bulgular ve Görüşler

Araştırmaya katılım sağlayanlara uygulanan yaklaşımların denetimin verimliliğine katkı sağlayıp /sağlamadığına yönelik sorulan soruya ilişkin verilen yanıtlara bakıldığında yeni yaklaşımlara yeterli düzeyde uyum sağlanması, yeterli bilgi birikimi ve eğitimi, tarafsızlığa dikkat edilmesi gibi hususlara değinen akademisyenlerin verimliliğe olumlu açıdan katkı sağladığı yönünde bir görüş birliği içinde oldukları tespiti yapılmıştır. Bu kapsamda ilgili soruya ilişkin bazı akademisyen görüşleri aşağıdaki gibidir:

Katılımcı AK1: "*Verimliliğin elimizdeki girdi ile maksimum çıktının elde edilmesi olduğunu düşünürsek denetimde de teknolojik yeniliklerin denetim süreçlerine denetim raporlarına katkısının maksimum seviyede olduğu söylenebilir özellikle bilgi teknoloji ürünlerinin kullanımı sayesinde tarafsızlık objektiflik önemli ölçüde sağlanabileceği için verimliliğin de artması mümkündür*."

Katılımcı AK3: "*Verimlilik en az kaynak ile maksimum çıktının elde edilmesi şeklinde tanımlanmaktadır. Teknolojik gelişmeler denetimde insan kaynağına olan ihtiyacı kayda değer oranda azaltmakta ve maliyetleri düşürerek çıktının niceliğini ve niteliğini artırmaktadır. Daha kısa sürede ve daha az sayıda insanla nispeten daha verimli denetim faaliyetleri sürdürülebilmektedir.*"

Katılımcı AK9: "*Yeni yaklaşımlara uyumun sağlanmasıyla birlikte denetimde verimlilik artmaktadır.*"

4.6.7. Denetim Faaliyetlerinde Çağdaş Yaklaşım ve Teknoloji Kullanımlarının Denetçilerin Yerini Alabileceği Diğer Bir İfadeyle İstihdamı Azaltacağı Yönündeki Düşüncelerin Tespitine İlişkin Bulgular ve Görüşler

Bu konuyla ilgili katılımcı görüşleri değerlendirildiğinde, akademisyenlerden 8'i istihdamı azaltmayacağı; 6'sı ise azaltacağı yönünde görüş bildirmiştir. Ancak burada özellikle üzerinde durulan konu; denetçilerin kendilerini sürekli yenilemeleri, analitik düşünebilmeleri, bilgi teknolojisiyle ortaya çıkan uygulamaları yorumlayabilmeleri halinde insana olan ihtiyacın asla azalmayacağı yönündeki görüşlerdir. Akademisyenlere ait diğer görüşlerin bazıları aşağıdaki gibidir:

Katılımcı AK1: *"Evet genelde literatürde bu yönde değerlendirmeler mevcuttur ancak Çağdaş Yaklaşım ve Teknoloji Kullanımlarının denetçilerin yerini alabileceğini düşünmüyorum denetim mesleği yine devam edecektir. Denetçilerin yeni denetim modellerine göre kendilerini güncellemeleri klasik denetim yöntemlerinden uzaklaşarak bilgi teknolojileri ile yapılan denetim süreçlerine kendilerini adapte edebilmeleri kullanılan dijital uygulamaları çok iyi bir şekilde bilmeleri analitik düşünebilen yorumlayabilen yetkinliklere sahip olabilmeleri istihdamı kısmen de olsa azaltabilir ancak nihayetinde bilgi teknolojisi ürünlerinin sunduğu bilgileri yorumlayan bilgiye katma değer sağlayan iş gücüne sürekli ihtiyaç olacaktır."*

Katılımcı AK3: "*Teknolojinin insan kaynağına olan ihtiyacı önemli ölçüde azaltacağının yadsınamaz bir olgu olduğunu söylemek mümkündür. Ancak denetimde tamamen insansız, sadece robot yazılımlar veya uygulamalar ile faaliyetlerin yürütülmesinin de olanak dahilinde olmayacağı açıktır. Akıllı makineler ancak insanların geliştirdiği algoritmalar kadar bir yargı kabiliyeti taşımaktadır. İnsanın davranışlarının karmaşıklığı dikkate alındığında bazı denetim türlerinde insana olan ihtiyacın devam edeceği hatta artacağı dahi söylenebilir. Uyum denetiminde insana olan ihtiyaç minimum seviyeye inebilir. Çünkü buradaki süreçler yorumsal veya yargısal süreçlerin dışında tutularak net olarak tanımlanabilir. Ancak insan davranışlarının ön planda olduğu ve güçlü yargısal becerilere gereksinim duyulan hile veya suiistimal denetiminde insana olan ihtiyaç azalmayacak sadece insan kaynağının yetkinlik havuzunda önemli değişiklikler ortaya çıkacaktır.*"

Katılımcı AK5: "*İstihdamı azaltabilecektir. Bununla birlikte tamamen yok olmaktan ziyade istihdam bir dönüşüm geçirecektir. Denetçilerin daha fazla yazılım, kodlama, siber güvenlik vb. teknik donanımlara sahip olmaları gerekecektir.*"

Katılımcı AK10: *"Tamamen katılıyorum. İstihdamı azaltabileceği gibi, muhasebe bürolarının açılmasını önemli ölçüde azaltacaktır. Üniversitelerde muhasebe bölümlerinin kapanmasına neden olacak bu kapanmalar orta öğretime kadar inecektir."*

Katılımcı AK11: *"Bir ihtimal istihdam edilen denetçi sayısında azalma söz konusu olabilir ancak her şartta ve koşulda, teknoloji ne kadar ilerlerse ilerlesin, bizim yaptığımız işlerin büyük bir bölümünü yapay zekâ yerine getirsin yine denetçi muhakemesine ihtiyaç söz konusu olacaktır. Bu muhakemenin bir teknoloji ile sağlanmasının mümkün olamayacağını düşünüyorum. Özellikle hile bağlamında bu durumun geçerliğinin daha yüksek olduğunu düşünmekteyim."*

Katılımcı AK12: *"Denetçiler yeterli gelişim ve eğitim sürecini tamamlamazlarsa bu sürecin gerisinde kalabilirler. Şu anki mevcut durum geçmişle kıyaslanınca istihdam açısından azalma söz konusudur. Ancak bu yaklaşımların/uygulamaların yönetilmesi bakımından nitelikli işgücüne ve eğitime ihtiyaç olacağı için bu alanda çalışanların bu konudaki adaptasyonlarının sağlanmasıyla ve kendilerini geliştirmeleri ile bu olumsuzluk ortadan kaldırılabilir. Tamamen yerini alma gibi bir durum şuan için söz konusu olmayacağı düşüncesindeyim. İnsan faktörünün payı hiçbir işte geri plana itilmeyeceği gibi denetim alanında da itilemez.*"

Araştırmanın sonunda katılımcılara **"***Konuyla ilgili görüş ve önerileriniz var ise paylaşır mısınız?*" şeklinde bir yönlendirme de yapılmış; konuyla ilgili değinilen diğer görüşlere aşağıda yer verilmiştir.

Katılımcı AK2: **"***Birçok alanda olduğu gibi denetim alanında da güncel yaklaşımların uygulanmasının denetim sürecine olumlu etkilerinin olabileceği gibi olumsuz etkilerinin olması da mümkündür. Diğer alanlarda da geçerli olmak üzere denetim alanında da eğitim ve yeterlilik önemli bir paya sahiptir. Konuya ilişkin hem eğitim kurumlarında, hem denetim alanında çalışanlarda hem de denetim kurumları açısından yeterli bilgi, tecrübe ve eğitim düzeyine sahip olunması gerekliliktir. Bu anlamda bir bütün olarak günümüz şartlarının sunduğu gerekliliklere yönelik hazırlıkların yapılması, ihtiyaçların net bir şekilde belirlenmesi ve bu ihtiyaçlara yönelik desteğin sağlanması ile yaşanan bu değişim sürecine uyum sağlanabilir. Olumsuz etkiler tamamen ortadan kaldırılamamış olsa da daha az seviyeye indirilebilir. Çalışmanızın alana katkı sunması dileğiyle, başarılar dilerim."*

Katılımcı AK3: "*Büyük veri ve yapay zekâ alanında yaşanan gelişmeler iç denetim faaliyetlerinde köklü bir değişime öncülük etmektedir. IDEA ve GALVANİZE gibi veri analitiği esaslı genelleştirilmiş denetim yazılımları (GAS'lar) iç denetim başta olmak üzere uyum, risk ve yönetim konularında firmalara etkin çözümler sunmakta ve günden güne daha fazla tercih edilmektedir. Bu eğilimin artarak devam edeceği, diğer bir ifade ile geleceğin iç denetiminin merkezinde özünü büyük verinin ve veri analitiğinin oluşturduğu bilgi teknolojilerine dayalı denetim teknikleri ve araçlarının olacağı söylenebilir."*

Katılımcı AK5:" *Denetimde bu teknolojilerin kullanılması için kurumların ekonomik, teknik ve personel anlamında yatırım yapmaları, gelişimlere sürekli açık bir şekilde davranmaları gerekir."*

5. SONUÇ

Dijitalleşmenin artık bir seçim olmadığı çağımızda, değişim ve dönüşüme adaptasyon sağlamak ve çalışmalara bu yönde değer katmak zorunluluk haline gelmiştir. Aksi durumda, teknolojiye ve dijital dönüşüm sürecine ayak uyduramayan bütün işletmeler ve kurumlar bu çemberin çok dışında kalarak yok olmaya mahkûm olacaktır. İş hayatını etkileyen güncel ve teknolojik gelişmelerin tümü denetim alanında faaliyette bulunan kişi/kurum/kuruluşların da çalışmalarını etkileyerek gerek denetim sürecine gerekse denetim kalitesine yansıyacaktır. Bu nedenle her alanda olduğu gibi denetim alanında da ortaya çıkan güncel yaklaşım ve teknolojik yeniliklerin kullanımıyla ön plana çıkan dijital akım yeni nesil teknolojilere daha kolay uyum sağlanmasına destek olacaktır. Yeni nesil teknolojilerin kullanımıyla dinamik yapıya sahip, öğrenen ve etkileşimi daha başarılı bir şekilde gerçekleştiren sistemin oluşması sağlanacaktır. Yapay zekâ, dijital ikiz, blok zincir, bulut bilişim, siber güvenlik bu kapsamda son yıllarda denetim alanında ortaya çıkan güncel yaklaşım ve teknolojik yeniliklerden bazılarıdır. Bu yeniliklerin etkin ve verimli bir şekilde kullanımının denetçilerin tutumlarına, denetimin işleyişine, denetim kalitesine ve denetim sürecine etkisinin olduğu açıkça görülmektedir.

Bu çerçevede bu çalışmadaki amaç, denetimde ortaya çıkan güncel yaklaşımlar ve teknolojik yeniliklerin denetim sürecine olan etkilerinin ortaya çıkarılmasıdır. Bu doğrultuda çalışmada akademisyen görüşlerinin incelenmesine yönelik nitel bir araştırma yapılmıştır. Araştırmada akademisyenin konuyla ilgili görüşlerine yer verilerek; değerlendirmeler yapılmıştır.

Araştırma sonucunda, denetimde teknolojik gelişmelerden yeterli düzeyde yararlanıldığına yönelik araştırma sorusuna 9 akademisyen olumlu yanıt verirken; 5 akademisyenin ise olumsuz yanıt verdiği görülmektedir. Teknolojiden yeterli düzeyde yararlanılmasında bazı alanlarda geliştirilen programların (iç denetim alanında "İçDen" yazılım programının; sağlık sektöründe "deniz" yazılım programının kullanılması gibi) katkısının olduğu yönünde fikirler beyan edilmiş olsa da hala kısıtlılıkların olduğu görüşüne de yer verilmiştir. Yeni teknolojilerin maliyetli olmasından kaynaklı eski teknolojilerin kullanılması da bir diğer eksiklik olarak görülmektedir. Bu çerçevede katılımcıların bilgisayar destekli teknolojilerin kullanımının en üst düzeye çıkarılması ve işletmelerin denetim metodolojilerini teknoloji tabanlı olarak geliştirmeye yönelmeleri gibi zorunlukların olduğu ortaya çıkmıştır.

Araştırmada denetimde teknolojik gelişmelerin kullanılması ile zaman tasarrufu, maliyetlerde azalma, kayıtlarda ortaya çıkan hata ve hilelerin daha kolay tespit edilmesi gibi üstünlükler elde edilirken güvenlik zafiyetinin oluşması, siber saldırılara uğramada yaşanan sıkıntılar, iletişim eksikliğine ortam hazırlaması gibi sakıncalarının olduğu da ortaya çıkmıştır. Araştırmada elde edilen bir diğer sonuç ise, denetimde kullanılan teknolojik gelişmelerin bazen hata ve hilelerin tespitinde insan faktöründen daha etkili olduğu; bu durumun ise denetim kalitesine ve sürecine olumlu yansıdığı sonucudur. Şeffaf raporlama sisteminin gelişmesiyle daha kaliteli denetim faaliyetleri oluşturulacak, zamandan tasarruf ile denetim süreci kısalacak böylece denetime olan güven artacaktır. Çalışmada denetim faaliyetlerini gerçekleştiren denetçilerin, kurum ya da kuruluşların denetim alanındaki güncel yaklaşım ve teknolojik yeniliklere uyum sağlayamadıkları yönünde görüş birliğinin ortaya çıktığı bu konuda meslek odalarının ve diğer ilgili kuruluşların eğitim desteği vermesi, çalışanların ise bu tür eğitimlere katılım sağlayarak, sürece daha kolay adapte olmalarının kaçınılmaz olduğu ortaya çıkmıştır. Ayrıca kurumların ve işletmelerin bu konuyla ilgili yatırımlarını artırmaları gerektiği gelişen teknolojilere uyum sağlamanın denetimde verimliliği artırdığı yönünde görüşlerin olduğu görülmektedir. Çalışmadan elde edilen bir diğer sonuç ise, yaşanan gelişmelerin risk değerlendirmesi konusunda katkı sağlayacağı, firmalara risk ve yönetimi çerçevesinde etkin çözümler sunacağıdır.

Denetimde ortaya çıkan yaklaşımların ve gelişmelerin insana olan ihtiyacı azaltacağına yönelik düşüncelerin 6 katılımcı tarafından kabul gördüğü; 8'i tarafından ise kabul görmediği sonucu ortaya çıkmıştır. Teknolojinin gelişmesiyle denetimde istihdamın azalabileceği gerçeği olsa da denetçilerin yerinin asla doldurulamayacağı görülmektedir. Çalışmada özellikle katılımcıların değindiği önemli noktalardan biri de denetim faaliyetlerine büyük katkı sağlayan iç denetim faaliyetlerinin giderek yaygın hale gelmesi ve teknoloji kullanımının iç denetimde yaygınlaşmasıdır.

Sonuç olarak denetimde teknolojinin ve ortaya çıkan güncel yaklaşımların denetim kalitesine, verimliliğine ve sürecine etkilerinin üst düzeyde olduğu görülmekte; denetçilerin dijital dönüşüm sürecine ayak uydurabilmeleri için, KGK, meslek odaları vb. tarafından verilen mesleki eğitimleri, sempozyum, kongre gibi çalıştayları takip etmeleri ve değişime açık olmalarının kaçınılmaz olduğu sonucu yapılan çalışma sonucunda ortaya çıkmaktadır. Bu konuya ilişkin çalışma yapacak olan araştırmacılar, çalışmalarına farklı örneklemler ve analiz yöntemlerini kullanarak (nicel veri yöntemleri vb.) yön verebilirler.

.Araştırmada kullanılan araştırma formu, Bitlis Eren Üniversitesi Etik İlkeleri ve Etik Kurulu tarafından 15.02.2022 tarihinde 22/02-4 sayılı ve E.1769 evrak kayıt kararıyla uygun görülmüştür. (Sayı: E-84771431-050.03-40650)

Kaynakça

Acar, D., Öztürk, M., & Usul , H. (2016). Dijital Ortamda Denetim: Sürekli Denetim. *Süleyman Demirel Üniversitesi, İktisadi ve İdari Bilimler Fakültesi Dergisi, 21*(5), 1561-1571.

Acar, D., Öztürk, M., & Usul, H. (2016). Dijital Ortamda Denetim: Sürekli Denetim. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 21*(5), 1561-1571.

ACFE. (2016). *Report to the Nation on Occupational Fraud and Abuse.* USA: ACFE.

Ajah, I., & Inyiama, C. (2011). Loan Fraud Detection and IT-Based Combat Strategies. *Journal of Internet Banking and Commerce,, 6*(2), 1-13.

Akbank. (2016). *Rüşvet ve Yolsuzlukla Mücadele Politikası.* İstanbul : Akbank .

Akdağ, F. (2017). İş Güvenliği Hizmetinin Dışarıdan Temini ile İşletme İçinden Sağlanmasının Çalışan Verimliliği Üzerine Etkisi: İnşaat Sektöründe Bir Uygulama. *Ankara: Ufuk Üniversitesi Sosyal Bilimler Enstitüsü*.

Akduran, E. (2019). Çalışan Dayanaklılığının İşletmelerde Verilmlilik Algısına Etkisi . *Edirne: Trakya Üniversitesi Sosyal Bilimler Enstitüsü (Yayımlanmış Yüksek Lisans Tezi)*.

Akgün, Z. (2018). Dijital Pazarlamada C Kuşağının Dijtal Ürünleri Benimseme Düzeyi Farklılıklarının Belirlenmesine Dair Bir Alan Araştırması (Yayımlanmış Doktora Tezi). *Çorum: Hitit Üniversitesi Sosyal Bilimler Enstitüsü* .

Aksoy, T., & Gurol, B. (2021). Artificial Intelligence in Computer-Aided Auditing Techniques and Technologies (CAATTs) and an Application Proposal for Auditors. Auditing Ecosystem and Strategic Accounting in the Digital Era: Global Approaches and New Opportunities, T. Aksoy & U. Hacioglu (Eds.). Springer, Cham, 361-384. Switzerland. https://doi.org/10.1007/978-3- 030-72628-7

Akyel, R., & Köse , H. (2010). Kamu Yönetiminde Etkinlik Arayışı: Etkin Kamu Yönetimi İçin Etkin Denetimin Gerekliliği. *Türk İdare Dergisi* .

Apilioğulları, L. (2018). *Dijital Dönüşümün Yol Haritası: Endüstri 4.0: Değişimin Değiştirdikleri* . İstanbul : Agora Kitaplık.

Arslan, A. (2021, 01 03). https://ms.hmb.gov.tr/: https://ms.hmb.gov.tr/uploads/2019/09/Kamu-Harcamalari-_A.-ARSLAN_-2.pdf adresinden alındı

Artun, T. (1980). *İşlevi-Gelişimi-Özellikleri Ve Sorunlarıyla Türkiye'de Bankacılık.* İstanbul : Tekin Yayınevi.

Association, A. A. (1973). *A Statement of Basic Auditing Concepts:Studies in Accounting* . American: ASOBAC.

Ataman, B., & Aydın, R. (2017). Hile Denetimi ve Denetçilerin Hile Tespitine Yönelik Bir Araştırma. *Marmara Business Review, 2*(1), 1-23.

Ayaz, M. (2011). Bankalarda İç Denetim Yaklaşımları ve Bir Uygulama Örneği . *İstanbul: Marmara Üniversitesi Sosyal Bilimer Enstitüsü* .

Aydın, N. (2006). *Bankacılık Uygulamaları* . Eskişehir : Anadolu Üniversitesi Yayınları .

Aytar, O. (2022). Kurumsal Yönetim Sistemi ve İlkelerinin Kamu Kesiminde İç Denetim Perspektifi İle Değerlendirilmesi. *Denetişim Dergisi*(24), 5-21.

B. Wang, Liu, , Y., Qian, , J., & Parker, S. (2021). Achieving Eeffective Remote Working During the COVID-19 Pandemic:: A Work Design Perspective. *Applied Psychology,, 70*(1), 16-59.

Baird, J., & Zelin , R. (2008). Understanding Employee Perceptions of Fradulent Activitiesand Their Propensity to Report Those Activities Using Anonymous Tip Lines: The Influence of Fraud Type,Propetrator Gender, and Observer Demographics. *Southern Business Review.*

Bakırtaş, T., & Ustaömer, K. (2019). Türkiye'nin Bankacılık Sektöründe Dijitalleşme Olgusu. *Ekonomi, İşletme ve Yönetim Dergisi, 3*(1), 1-24.

BBVA. (2015). *Turkish Banks' Digitalisation, Digital Economy Outlook.* BBVA.

Bozkurt, N. (2016). *İşletmelerin Kara Deliği Hile: Çalışan hileleri (6.Baskı).* İstanbul: Alfa Yayınları.

Bozkurt, P. (2013). Denetim ve Denetim Anlayışındaki Gelişmeler. *Denetişim Dergisi*(12), 56-62.

Bulut, E., & Çizgici Akyüz , G. (2020). Türkiye'de Dijital Bankacılık ve Ekonomik Büyüme İlişkisi. *Marmara Üniversitesi İktisadi ve İdari Bilimler Dergis, 42*(2), 223-246.

Büyüköztürk, Ş., Çakmak , E., Akgün , Ö., Kadeniz , Ş., & Demirel , F. (2014). *Bilimsel Araştırma Yöntemleri.* Ankara : Pegem Yayıncılık.

Büyüköztürk, Ş., Kılıç Çakmak, E., Akgün , Ö., Karadeniz , Ş., & Demirel , F. (2014). *Bilimsel Araştırma Yöntemleri* . Ankara : Pegem Yayıncılık.

Celayir, D., & Celayir , Ç. (2020). Dijitalleşmenin Denetim Mesleğine Yansımaları. *Avrasya Sosyal ve Ekonomi Araştırmalar Dergisi, 7*(6), 128-148.

Ciğer, A., & Kınay , B. (2018). Bağımsız Denetim Firmalarının Bulut Bilişim Uygulamalarını Benimseme Düzeylerine Yönelik Nitel Bir Araştırma: Antalya İli Örneği. *Muhasebe Bilim Dünyası Dergisi, 20*(3), 629-649.

COSO. (2010). *Fraudulent Financial Reporting: 1998-2007, An Analysis Of U.S. Public Company.* COSO .

Çakmak, T. (2016). "Türkiye'de Kültürel Bellek Kurumlarında Dijitalleştirme ve Dijital Koruma Politikaları: Bir Model Önerisi (Yayımlanmış Doktora Tezi) . *Ankara: Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü* .

Çankaya, F., & Gerekan, B. (2009). Hile Denetçiliği Mesleği ve Sertifikalı Hile Denetçiliği Mesleki Standartları ve Ahlak Kuralları. *Muhasebe ve Denetima Bakış Dergisi*, 93-108.

Çatıkkaş, Ö., & Çalış , E. (2010). Hile Denetiminde Proaktif Yaklaşımlar. *Muhasebe ve Finansman Dergisi*(45), 146-156.

Çelik, S., & Mangır , F. (2020). Bankacılık Sektörünün Dijitalleşmesi:Dünya'da ve Türkiye'de Durum Analizi. *Cyberpolitik Journal, 5*(10), 260-282.

Deloitte. (2017). Blockchain Technology and Its Potential Impact on the Audit and Assurance: https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/blockchain-technology-and-its-potential-impact-on-the-audit-and-assurance-profession.pdf. adresinden alındı

Demirel, A. C. (2017). Dijital Bankacılık ve Türkiye'dek Mevcuti Durumun Analizi. *Ankara: Başkent Üniversitesi Sosyal Bilimler Enstitüsü*.

Demirez, D., Gür , D., & Yaşa Özeltürkay , E. (2021). Bankacılık Sektöründe Dijital Dönüşüm: Açık Bankacılık ve Uygulamalarına İlişkin Kavramsal Bir Araştırma. *Tarsus Üniversitesi Uygulamalı Bilimler Dergisi, 1*(1), 10-28.

Dengler, K., & Matthes, B. (2018). The Impacts of Digital Transformation on the Labour Market: Substitution Potentials of Occupations in Germany. *Technol. Forecast. Soc.*(137), 304-3016.

Dijital Dönüşüm. (2021). 07 30, 2021 tarihinde https://dijitaldonusum.com/dijital-donusumun-faydalari-nelerdir/. adresinden alındı

Dijital Dönüşüm ve Verimlilik. (tarih yok). 08 02, 2021 tarihinde https://fintechistanbul.org/2018/12/23/bankalarin-gelistirmek-gereken-3-verimlilik-alani/ adresinden alındı

Doğan, S., & Kayakıran , D. (2017). İşletmelerde Hile Denetiminin Önemi. *Maliye Finans Yazıları Dergisi* , 167-188.

Dönmez, A., & Çavuşoğlu, K. (2015). Hilelerin Ortaya Çıkarılması Bakımından Bağımsız Denetim ile Adli Muhasebenin Karşılaştırılması. *Journal of Accounting, Finance and Auditing Studies, 1*(3), 34-67.

Dönmez, A., & Karausta , A. (2011). "Çalışanların Mesleki Hile Algısı ve İhbar Hattı Kullanarak Rapor Etme Eğilimleri Üzerine Akdeniz Üniversitesi İktisadi ve İdari Bilimler Fakültesi'nde Yapılan Bir Araştırma. *Mali Çözüm Dergisi*.

Durmuş, Ü. K. (2015). Mobbingin Çalışan Verimliliği Üzerindeki Etkileri: Sakarya İmalat Sanayisinde Bir Araştırma(Yayımlanmış Yüksek Lisans Tezi). *İstanbul: Maltepe Üniversitesi Sosyal Bilimer Enstitüsü*.

Emir, M. (2008). Hile Denetimi. *Mali Çözüm Dergisi*(38).

Erdoğan, E. (2020). Dijital Muhasebe Uygulamaları Kullanımının Teknoloji Kabul Modeli İle İncelenmesi:. *Muhasebe Meslek Mensupları Üzerine Bir Araştırma. İnönü Üniversitesi Sosyal Bilimler Enstitüsü (Yayımlanmış Yüksek Lisans Tezi).*

Erturan, İ., & Ergin , E. (2018). Dijital Denetim ve Dijital İkiz Yöntemi. *Muhasebe Bilim Dünyası Dergisi, 20*(4), 810-830.

Ghasemi, M., Shafeiepour, V., Aslani, M., & Barvayeh, E. (2011). The Impact of Information Technology (IT) on Modern Accounting Systems. *Procedia-Social and Behavioral Sciences*(28), 112-116.

Gökbayrak, S. (2020). Bağımsız Denetim Sürecinde Denetçilerin Denetçilerin Denetim Riskine Yönelik Yaklaşımlarının Araştırılması . *Kırşehir Ahi Evran Üniversitesi Sosyal Bilimler Enstitüsü* .

Gökoğlan, K. (2019). Bağımsız Denetimin Kalitesi Açısından Denetimin Katma Değeri:Yatırım Kuruluşları Üzerine Bir Araştırma . *Nevşehir: Hacı Bektaş Veli Üniversitesi Sosya Bilimler Enstitüsü* .

Gökten, S., & Özdoğan , B. (2019). The Doors are Openning for the New Pedigree: AFuturistic View for the Effects of Blockchain Technology on Accounting Application. *Digital Business Strategies in Blockchain Ecosystems, Contributions to Management Science.*(Springer), 425-438.

Gülbahar, Ç., & Koşar, D. (2020). Özel Okul Yöneticilerinin Yetenek Yönetimine İlişkin Görüşlerinin İncelenmesi. *Eğitimde Nitel Araştırmalar Dergisi, 8*(3), 1000-1028.

Gümüş, U., & Göğebakan , H. (2016). Muhasebe Hata ve Hileleri ile Muhasebe Mesleğinde Etik, Aydın İlinde Muhasebeciler Üzerine Bir Araştırma. *Uluslararası İşletme, Ekonomi ve Yönetim Perspektifleri Dergisi, 1*(3), 12-27.

Güredin, E. (2010). *Denetim* . İstanbul : Beta Yayınevi .

Hacıhasanoğlu, T., & Karaca , N. (2015). Potansiyel Muhasebe Meslek Mensuplarının Hile Algısı Üzerine Bozok Üniversitesi'nde Yapılan Bir Araştırma. *Niğde Üniversitesi İİBF Dergisi, 8*(1), 117-130.

Halbouni, S. (2015). The role of auditors in preventing, detecting and reporting fraud The case of the United Arab Emirates (UAE). . *International Journal of Auditing, 19*(2), 117–130.

Kaban, İ., & Gül , M. (2019). Bankalarda Hile Denetimi: Merkezden Sürekli Denetimin Şube Faaliyetlerine Etkisi Üzerine Nitel Bir Araştırma. *Istanbul Business Research*(1), 1-33.

Kaban, İ., & Gül , M. (2019). Bankalarda Hile Denetimi: Merkezden Sürekli Denetimin Şube Faaliyetlerine Etkisi Üzerine Nitel Bir Araştırma. *Istanbul Business Research, 48*(1), 113-143.

Kahyaoğlu, S. B., & Aksoy , T. (2021). Artificial Intelligence in Internal Audit and Risk Assessment : Financial Ecosystem and Strategy in the Digital Era.Ü. Hacıoğlu, & T. Aksoy (Eds). *Springer.Cham.* 179-192. Switzerland. https://doi.org/10.1007/978-3-030-72624-9-8.

Karabayır, M., & Cengiz , S. (2016). Muhasebe Hileleri Yoluyla Yapılan Yolsuzluklarda Bağımsız Denetimin Sorumluluğunun Araştırılması: Kuzeydoğu Anadolu Bölgesi Uygulaması. *Kafkas Üniversitesi İİBF Dergisi, 7*(14), 701-709.

Karacan, S., & Uygun , R. (2012). *Denetim ve Raporlama (1.Baskı).* Kocaeli : Umutttepe Yayınları .

Karaduman, İ. (2017). Muhasebe Denetiminde XBRL ve Yapay Zekâ Kullanımının Denetim Sürecine Etkisi ve Uzman Sistemler Uygulaması . *Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü (Yayımlanmış Dokotra Tezi)*.

Karahan, M., & Çolak , M. (2019). Hile Önleyici Olarak Sürekli Denetim Verimliliği. *Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi, 21*(2), 561-572.

Kars, B. N. (2021). Edge Computing Security With an IoT Device. *Journal of Emerging Computer Technologies, 1*(1), 14-17.

Kazan, G. (2021). Hile Üçgeni, Hile Elmesı ve Hile Beşgeni: Hile Eylemlerinin Nedenlerine İlişkin Teorilerle Kavramsal Bakış . *Muhasebe ve Denetime Bakış* , 245-258.

Kebeli, A. (2020). Kamu İç Denetiminde Performans Denetimin Yeri. *Denetişim*(20), 5-34.

Kenger, E. (2001). *Denetçi Yardımcıları Eğitim Notu.* Ankara : YDK Yayınları.

Kıızl, C., Akman , V., & Korkmaz , H. (2015). Marmara Bölgesinde Muhasebe Denetim Mesleğinin Önemi Üzerine Bir Araştırma. *Akademik Sosyal Araştırmalar Dergisi, 3*(10), 193-211.

Kiracı, M. (2013). Hileye Yönelik Uluslararası Kuruluşların Hazırladığı Raporların Bağımsız Denetim Açısından Değerlendirmesi. *Ankara SMMMO, Muhasebe ve Vergi Uygulamaları Dergisi* , 87-106.

KMPG. (2017). *Clarity on Dynamic Audit.* https://assets.kpmg/content/dam/kpmg/ch/pdf/clarity-on-dynamic-audit-en.pdf, adresinden alındı

Kranacher, M., & Riley , R. (2020). *Forensic Accounting and Fraud Examination.* Wiley .

Manita, R., Ellomal , N., Baudier,, P., & Hikkerova,, L. (2020). The Digital Transformation of External Audit and Its Impact on Corporate Governance. *Technological Forecasting and Social Change, 150*(119), 1-10.

Mengi, B. (2012). Hile Denetiminde Yetkinliklerin Değerlendirilmesi-Hile Karosu. *Mali Çözüm Dergisi* , 113-128.

Miles, M., & Huberman, A. (2015). *Nitel veri analizi (S. Akbaba ve A. A. Ersoy, Çev.).* Ankara : Pegem Akademi.

Miles, M., & Huberman, M. (1994). *An Expanded Sourcebook Qualitative Data Analysis.* Sage .

Mucuk, İ. (2011). *Modern İşletmecilik.* İstanbul : Türkmen Kitabevi.

Mullan, J., Bradley, L., & Loane , S. (2017). Bank Adoption of Mobile Banking: Stakeholder Perspective. *International Journal of Bank Marketing*, 1147-1154.

Murphy, M. (2015). *How the Internet of Things will Impact CPAs,*. https://www.aicpastore.com/Content/media/PRODUCER_CONTENT/Newsletters/Articles_2015/CPA/MAY/impact_CPAs.jsp, adresinden alındı

Oğuz, F. (2007). İşletmelerde Verimlilik Arttırımında İş Ölçümü Tekniği ve Bir Uygulama . *Ankara: Gazi Üniversitesi Sosyal Bilimler Enstitüsü* .

Okutmuş, E., & Uyar , S. (2014). "Konaklama İşletmelerinde Yiyecek-İçecek Departmanında Yapılan Bir Hilenin Tespiti: Vaka Analizi. *Mali Çözüm Dergisi*(121), 35-54.

Omarani, A. (2018). Banks And Fintechs: How To Develop a Digital Open Banking Approach For The Bank's Future. *International Business Research, 11*(9), 23-36.

Öğütçü, N. (2019). Dijitalleşmenin Türkiye Bankacılık Üzerindeki Etkileri (Yayımlanmış Yüksek Lisans Tezi). *İstanbul: Maltepe Üniversitesi Sosyal Bilimler Enstitüsü*.

Özdemir, İ., & Sarıoğlu, Ş. (2018). Denetimlerde Büyük Veri Kullanımı Ve Üzerine Bir Değerlendirme. *Gazi Üniversitesi Fen Bilimler Dergisi, 6*(2), 471-479.

Özen, A., & Gürel , F. (2020). Kamu Denetiminde Dijital Dönüşüm: Dijital İkiz Yöntemi. *İzmir Sosyal Bilimler Dergisi, 2*(1), 16-23.

Özkul, F. U., & Alkan , B. (2020). Dijital Çağda Muhasebenin Dönüşümü: Blockchain Teknolojisinde Muhasebe ve Mali kotroller. *Muhasebe Bilim Dünyası Dergisi, 22*(2), 218-236.

Öztoprak, Y. (2017). Denetimde Hata ve Hile, Önleme ve Tepit Yöntemleri ile Serbest Muhasebeci Mali Müşavirlerin Hata ve Hile İlgili Bilinç ve Tutumları . *İstanbul: Gelişim Üniversitesi Sosyal Bilimler Enstitüsü (Yayımlanmış Yüksek Lisans Tezi)*.

Öztürk, M. S. (2021). Denetimde Yenlilikçi Yaklaşım Modeli. K. (Ed.) DemirYürek, B. Türk, & A. Kahramanaoğlu içinde, *Girişimcilik ve Yenilikçilikte Güncel Yaklaşımlar 2* (s. 103-119). İstanbul: Efe Akademi.

Patton, M. (1990). *Qualitative Evaluation and Research Methods.Beverly Hills.* CA: Sage.

Pehlivanlı, D. (2011). *Hilde Denetimi, Metodloji ve Raporlama* . İstanbul : Beta Yayın .

Potton, M. (1990). *Qualitative Evaluation and Research Methods.* Beverly Hills. CA: Sage.

Rajdeepa, B., & Nandhitha, D. (2015). Fraud Detection in Banking Sector Using Data Mining. *International Journal of Science and Research, 4*(7), 1822-1825.

Ruyter, K., & Scholl, N. (1998). Positioning Qualitative Market Research: Reflections from Theory and Practice. *Qualitative Market Research: An International Journal, 1*(1), 7-14.

Salameh, R., Al-Weshah, G., Al-Nsour, M., & Al-Hiyari, A. (2011). Alternative Internal Audit structures and perceived effectiveness of ınternal audit in fraud prevention: Evidence from jordanian banking industry. *Canadian Social Science*, 40-50.

Serçemeli, M. (2018). Muhasebe ve Denetim Mesleklerinin Dijital Dönüşümünde Yapay Zekâ. *Turkish Studies, 13*(30), 369-386.

Sevim, T., & Ömür , G. (2015). Customer Perspective in Use of Internet Banking. *The International Journal of Human, Community&Technology, 1*(1), 1-8.

Sevimli, Ö. (2013). Sağlık Kurumlarında Veri Zarflama Analizi Tekniği ile Verimlilik Analizi. *İstanbul: Beykent Üniversitesi Sosyal Bilimler Enstitüsü (Yayımlanmış Yüksek Lisans Tezi)*.

Sultan, K., Ruhi, U., & Lakhani , R. (2018). Conceptualizing Blockchains:Conceptualizing Blockchains:and Application. *11th IADIS International Conference on Information Systems*, (s. 49-57). Canada .

Şengür, D. (2010). İşletmelerde Hile, Hilelerin Önlenmesi, Hileli Finansal Raporlama İle İlgili Düzenlemeler ve Bir Araştırma (Yayımlanmış Doktora Tezi). *İstanbul: İstanbul Üniversitesi Sosyal Bilimler Enstitüsü*.

Taş, O., & Mert, H. (2019). Denetimde Yapay Zekâ Uygulaması. *PressAcademia Procedia, 9*(1), 65-68.

Tekin, S. (2019). Bankacılıkta Dijital Gelişmeler ve Müşterierin Dijitalleşmeye Uyumu ve Analizi . *Konya: Necmettin Erbakan Üniversitesi Sosyal Bilimler Enstitüsü* .

Tor, S. S. (2011). Örgütlerde İş Tatminini Etkileyen DemografikFaktörler ve Verimlilik: Karaman Gıda Sektöründe Bir Uygulama. *Karaman: Karamanoğlu Mehmetbey Üniversitesi Sosyal Bilimler Enstitüsü (Yayımlanmış Yüksek Lisan Tezi)*.

Türk Dil Kurumu,Büyük Türçe Sözlük . (17.01.2021). www.tdk.org.tr. adresinden alındı

Ulucan Özkul, F., & Özdemir , Z. (2013). Çalışan Hilelerinin Önlenmesinde Proaktif Yaklaşımlar: Kurumsal İşletmelerde İnsan Kaynakları Yöneticileri Üzerine Nitel Bir Araştırma. *Marmara Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 10*(40), 75-89.

Wolfe, D., & Hermanson , D. (2004). The Fraud Diamond: Considering the Four Elements of Fraud. *CPA Journal* , 38-42.

Siriwardhana, Y., Porambage, , P., Liyanage, M., & Ylianttila, M. (2021). A Survey on Mobile Augmented Reality With 5G Mobile Edge Computing: Architectures, Applications and Technical Aspects. *IEEE Communications Surveys & Tutorials, 23*(2), 1160-1192.

Yel, T., & Atasoy, A. (2021). Dijitalleşmenin Bağımsız Denetime Yansımalarının Siber Güvenlik Yönünden Değerlendirilmesi. *Muhasebe ve Finansman Dergisi*(Özel Sayı), 439-458.

Yıldırım, A., & Şimşek , H. (2013). *Sosyal Bilimlerde Nitel Araştırma Yöntemleri.* Ankara : Seçkin Yayıncılık.

Yıldırım, A., & Şimşek , H. (2016). *Sosyal Bilimlerde Nitel Araştırma Yöntemleri.* Ankara : Seçkin Yayıncılık.

Yıldırım, A., & Şimşek, H. (2011). *Sosyal Bilimlerde Nitel Araştırma Yöntemleri,.* Ankara: Seçkin Yayıncılık.

Yumuşak, S. (2008). şgören Verimliliğini Etkileyen Faktörlerin İncelenmesine Yönelik Bir Alan Araştırması. *Süleyman Demirel Üniversitesi İBBF Dergisi, 13*(3), 241-251.

Yusheng, K., & Ibrahim , M. (2019). Service innovation, service delivery and customer satisfaction and loyalty in the banking sector of Ghana. *International Journal of Bank Marketing, 37*(5), 1215-1233.

Zager, L., Malis, S., & Novak, A. (2016). "The Role And Responsibility Of Auditors İn Prevention And Detection Of Fraudulent Financial Reporting. *Procedia Economics And Finance*, 693-700.

Zeybek, H. (2018). Dijital Bankacılık. *Mali Çözüm Dergisi, 28*(150), 79-107.

Zhang, C. (2019). Intelligent Process Automation in Audit. *Journal of Emerging Technologies in Accounting*, *16*(2), 69-88.

HAKEMLİ Denetişim
Ortak Aklın Harmanı

Kamu İç Denetçileri Derneği Meşrutiyet Caddesi Konur Sokak No: 36/6 Kızılay - ANKARA
www.kidder.org.tr/denetisim/ • denetisim@kidder.org.tr
ISSN 1308-8335
Yıl: 13, Sayı: 26, 32-44, 2022

Araştırma Makalesi

DENETÇİLERİN YAPAY ZEKÂ'YA YÖNELİK ALGILARININ DENETİM KALİTESİNE ETKİSİ ÜZERİNE BİR ARAŞTIRMA

(A RESEARCH ON THE EFFECT OF AUDITORS' PERCEPTIONS OF ARTIFICIAL INTELLIGENCE ON AUDITING QUALITY)

Eda KÖSE[1], Ali APALI[2] Mehmet Emin ALDEMİR[3]

ÖZ

Genel olarak iş ve profesyonel hizmetler için oyunun kurallarını değiştirebilen yapay zekâ uygulamalarının makine öğrenimi, veri madenciliği ve bilişsel hesaplamadaki hızlı gelişmeler ile birlikte gelecek dönemlerde büyük sıçrama yapacağı görülmektedir. Bu gelişmeler doğrultusunda yapay zekâ sistemleri, denetim sürecini de önemli ölçüde değiştirmiştir. Bazı denetçiler, değişen bu ortama uyum sağlamada yaşanacak zorluklar karşısında yapay zekâ sistemini geri adım olarak yorumlamaktadırlar. Bu araştırmada, denetçilerin yapay zekâ kullanımlarının kolaylığı, kullanışlılığı ve denetim kalitesine yönelik etkisine yönelik beklentileri araştırılacaktır. Bununla birlikte yapay zekâ kullanımı sonrasında denetim kalitesini etkileme durumu saptanacaktır. Bu doğrultuda yapay zekanın denetim kalitesine, kullanım kolaylığına ve denetim faaliyetlerine faydasını saptamak amacıyla üç hipotez oluşturulmuştur. Araştırmada, Antalya, Isparta ve Burdur illerinde faaliyet gösteren 251 bağımsız denetçiye online anket uygulanmıştır. Araştırmada, elde edilen veriler, SPSS 20 paket programı vasıtasıyla analiz edilmiştir. Araştırma verileri öncelikle güvenilirlik analizine tabi tutulmuştur. Araştırma kapsamında hipotezler regresyon yöntemi kullanılarak analiz edilmiştir. Araştırmada elde edilen bulgulara göre; denetim faaliyetlerinde yapay zekâ kullanımı ve kullanım kolaylığını denetim kalitesini arttırdığı ve yapay zekâ kolaylıkla kullanımı denetim faaliyetlerinde fayda sağladığı saptanmıştır.

Anahtar Kelimeler: Denetim, Denetim Kalitesi, Yapay Zekâ.

JEL Kodları: M40, M42, M49.

ABSTRACT

It is seen that artificial intelligence applications, which can change the rules of the game for business and professional services in general, will make a big leap in the future with the rapid developments in machine learning, data mining, and cognitive computing. Artificial intelligence systems have significantly changed the audit process in line with these developments. Some auditors interpret the artificial intelligence system as a step back in the face of difficulties in adapting to this changing environment. In this research, auditors' expectations for the ease, usefulness, and impact of artificial intelligence on audit quality will be investigated. In addition, after the use of artificial intelligence, it will be determined whether it affects the quality of the audit. In this direction, three hypotheses were formed to determine the benefit of artificial intelligence on audit quality, ease of use, and audit activities. In the research, an online questionnaire was applied to 251 independent auditors operating in the provinces of Antalya, Isparta, and Burdur. According to the findings of the study; In the research, the data obtained were analyzed by the SPSS 20 package program. The research data were first subjected to reliability analysis. Within the scope of the research, the hypotheses were analyzed by using the regression method. It has been determined that the use of artificial intelligence in audit activities and ease of use increase the quality of auditing and the ease of use of artificial intelligence is beneficial in audit activities.

Keywords: *Audit, Audit Quality, Artificial Intelligence.*

JEL Classification: *M40, M42, M49.*

- Eda KÖSE, Orcid Id: 0000-0002-9537-3672, edakose@nevsehir.edu.tr, Sorumlu Yazar
- Ali APALI, Orcid Id: 0000-0002-3521-0150, aapali@mehmetakif.edu.tr
- Mehmet Emin ALDEMİR, Orcid Id: 0000-0003-2378-5245, meminald@hotmail.com,

1. GİRİŞ

Günümüzün değişen dünyasında dijitalleşme ve teknoloji kullanımı işletmelerin faaliyetlerini daha verimli ve etkin hale getirmektedir. Bu bağlamda, öncelikli olarak endüstri 4.0 fikri sürekli araştırma ve tartışma konusu haline gelmiştir. İlerleyen dönemlerde ise yapay zekâ uygulamaları modern iş dünyasında önemli bir konu haline gelmiştir. Birçok işletme, yapay zekâ sistemlerinin iş yapma yolları üzerindeki potansiyelini tercih ederken, bazı firmalar ise yapay zekâ kullanımı ile ilgili olarak biraz daha çekingen yaklaşmışlardır. Denetim alanı da diğer sektörlerden farklı değildir. Denetim firmaları yaşanan bu değişiklikler karşısında daha hızlı, verimli ve doğru denetim kararları almak için ne gibi bir potansiyele sahip olduklarını görmek istemişlerdir (Heye, 2021, s. 2). Bu kapsamda, denetim firmaları, müşterilere riskten kaçınma ve maliyet tasarrufu sağlamak için yapay zekâyı öğrenme ve kullanmayı özümsemişlerdir. Bu yeni evrim, yapay zekâ tarafından kolaylaştırılan denetim olarak adlandırılmaktadır. Bu evrimin sonucu olarak muhasebe sisteminde de bazı değişiklikler olmuştur. Kâğıt üzerinde yapılan işlemler artık bilgisayar formatına dönüşmüş, dolayısıyla yapay zekâ kullanan işletmelerde çok sayıdaki verinin işlenmesini daha hızlı ve kolay hale getirmiştir. Bu sistem sayesinde, yevmiye kayıtlarının gözden geçirilmesi, sözleşmelerin okunması, hesapların belirli bir formata getirilmesi muhasebe ve denetim süreçlerinde harcanan zamanı azaltmıştır. Aynı zamanda sistem, yevmiye defterleri bir mekanizma tarafından kontrol edildiğinden dolayı yanlış beyanları ya da riskleri raporlama olanağı sunmaktadır (Gusai, 2019, s. 59).

Yapay zekânın denetim tarihine bakıldığında ilk girişimler 1980'lere kadar uzanmaktadır. Abdolmohammadi (1987), yapay zekânın başta karar destek sistemleri ve bilgi tabanlı uzman sistemler olmak üzere çeşitli bilgisayar tabanlı sistemlerin denetimde uygulama alanlarını belirlemiş ve her iki sistemi de kullanmanın denetim de karar verme etkinliğini arttırdığını ifade etmiştir. Denetim açısından yapay zekâ kullanımı ile ilgili olarak Borthick ve Weat (1987), *"denetimi planlayın, kanıtları toplayın, değerlendirin ve görüşler oluşturun"* şekilde bir sistemin oluşturulması halinde, denetim kalitesinin ve verimliliğin artacağını ifade etmişlerdir. Aynı zamanda yapay zekâ, denetim süreçlerinin ilk aşamalarında önemlilik derecesi önerebilir, iç kontrol kalitesini değerlendirebilir ya da karşılık tutarlarının yeterliliğini değerlendirebilir (Zemankova, 2019, s. 149).

İşletmelerin yapay zekâ sistemini kullanmaları; satış noktalarından stok sayımlarına kadar sürekli olarak büyük miktarda veriyi zamanında toplama ve üretme imkânı sağlayacaktır. Bununla birlikte yapay zekâ sistemleri kullanımı sosyal medya, haber kaynakları gibi dış kaynaklardan gelen bilgileri, kolayca erişilebilir ve analiz için hazır duruma getirebilecektir. Bu durum, denetim mesleğini bir adım ileriye götürebilecektir. İşleri bu kadar kolaylaştıracak sistemlerin kullanılması sonucunda geleneksel denetim prosedürlerinin etkisi de azalacak ve yeni sistem karşısında denetim faaliyetlerinin yürütülmesinin gözden geçirilmesi gerekecektir (Dai ve Vasarhelyi, 2016, s. 5). Ancak denetim mesleği, standart belirleme kurulları tarafından gerekli görülmedikçe ya da onaylanmadıkça yeni bir sistem ya da metodolojiyi benimsemeleri kolay olmayacaktır. Bu nedenle denetim mesleğinde, geleneksel uygulamaları yıkıcı etkisi olan yapay zekâ sistemini mevcut denetim standartlarına uyarlama zorluğu ile karşı karşıya kalınmıştır. Örnek olarak bağımsız denetçilerin yapay zekâyı benimseme noktasında isteksiz oldukları, bunun nedeni olarak ise mevcut denetim standartlarından kaynaklandığı görülmektedir. Günümüzde ise gerçek zamanlı dijital ekonomi karşısında uygulanan standartlar etkisiz hale gelmektedir. Bu standartlar, gerçek zamanlı olmasa bile daha yüksek seviyede güvence sağlamak için denetçilerin yapay zekâyı uygulamaları için bir takım düzenlenmeleri gerekmektedir. Bunun sağlanması durumunda; denetçi, bir işlemi manuel olarak incelemek yerine daha kısa sürede yapay zekâ ile gerçekleştirebilecek, zamanlarını el emeği olarak harcamak yerine çabalarını yapay zekâ tarafından üretilen sonuçlara odaklandırarak mesleki becerilerini daha iyi şekilde kullanma olanağı elde etmiş olacaktır (Vasarhelyi vd., 2010).

Yapay zekâ literatürü oldukça geniş kapsamlıdır. Algoritmik denemelerden çeşitli araştırma alanlarındaki uygulamalara kadar uzanmaktadır. Ancak, denetimde yapay zekâ araştırmaları sınırlıdır. Gillett ve Vasarhelyi (1993), denetçilerin denetim programlarına yardımcı olmak için denetim uzman sistemini geliştirmiş ve uzun yürütme sürecinin ilk adımlarını tanımlamışlardır. Omoteso (2012), denetçilerin denetim yargıları ile ilgili karar almada yapay zekâ sistemlerini kullanmalarının önemini tartışmıştır. BAI (2017), dört büyük uluslararası muhasebe firmasında denetim hizmetleri kapsamında yapay zekâ uygulamasını tanıtmış, yapay zekânın denetim sektöründen sorumlu düzenleyiciler üzerindeki etkisini analiz etmiştir. Gusai (2019), denetimde uzman sistemlerin ve sinir ağlarının kullanımına ilişkin araştırma çabalarını ve bunların sonuçlarını araştırmıştır. Ukpong vd. (2019), yapay zekâ teknolojilerinin muhasebe ve denetime uygulanma ihtiyacını gözden geçirmişlerdir. Zemankova (2019), en yeni trendler, fırsatlar ve tehditler dahil olmak üzere denetim ve muhasebe süreçlerinde yapay zekâ kullanımını analiz etmişlerdir. Albawwat ve Frijat (2021), Ürdün'de faaliyet gösteren denetim firmalarının denetim süreçlerinde yapay zekâ sistemlerini kullanmaya hazır olup olmadıklarını araştırmakla birlikte yapay zekâ türlerinin (destekli, artırılmış ve otonom) kullanım kolaylığı, kullanışlılık ve denetim kalitesine etkisini incelemişlerdir. Al-Sayyed vd. (2021), araştırmalarında denetçiler açısından yapay zekâ teknolojilerini kullanmalarının denetim kanıtları üzerindeki etkisine odaklanmışlardır.

Bu araştırmada, yapay zekâ uygulamalarının denetim faaliyetindeki gelişimi ve denetim üzerindeki etkisi dikkate alınarak güncel literatür ışığında, denetçilerin yapay zekâ kullanım kolaylığı, kullanım sonrasındaki fayda beklentileri ile yapay zekânın denetim kalitesine etkisine yönelik beklentilerinin tespit edilmesi amaçlanmıştır.

2. KAVRAMSAL ÇERÇEVE

Yapay zekâ, 1950'li yıllarda Alan Turing araştırmasından sonra kullanılan yaygın bir kavramdır. Bu araştırmada, bir makinenin zeki olabileceğini kanıtlayan bir test geliştirmiş ve insanla aynı iletişim davranışını sergilediği gözlemlenmiştir. Yapay zekâ kavramı; insan düşüncesini arttırma ya da simülasyon eden bilişsel yetenekleri ifade etmekte ve günlük yaşamda giderek daha fazla yer almaktadır (Alina vd, 2018, s. 441). Yapa zekâ, makinelere insan gibi hareket etme yeteneği vermeye odaklanan yeni bir otomasyon sistemidir. *"Makineleri akıllı hale getirmeye yönelik faaliyet, zekâ ve bir varlığın çevresinde uygun ve öngörülü şekilde çalışmasını sağlayan kalite"* olarak tanımlanmıştır (Etzioni ve Etzioni, 2017, s. 32). Kısaca yapay zekâ, insan aklını teknoloji yoluyla verimli çalışmaya dönüştürme yeteneğine sahip bilgisayar sistemidir.

Yapay zekâ uygulamaları ile muhasebecilik, denetçilik, taksi şoförlüğü, sekreterlik, uçuş ekibi ve pilotluk, ekonomistlik gibi mesleklerin işleri ve işin geleceği değişerek, mevcut iş faaliyetlerinin birçoğunun otomatik hale geleceği ifade edilmektedir. McKinsey (2017), saptam yaptığı araştırma sonucuna göre, 2025 yılına kadar işletmelerin üçte birinin işlerinin akıllı robotlar tarafından yapılacağını ıştır. Bununla birlikte sadece fabrika işleri değil aynı zamanda satış işleri, muhasebe, teknik işler, iletişim gibi işler de otomatik hale gelecektir. McKinsey, çalışmasında vurguladığı gibi fiili olarak yapılan işlerin %60'ı yapay zekâ aracılığıyla yapılacak ve faaliyetler otomatik olarak kolayca yapılacaktır sonucuna ulaşmıştır.

İşletmelerdeki bazı muhasebe faaliyetleri tekrarlanan mekanik bir yapıya sahiptir. Ancak bu faaliyetlerden elde edilen bilgiler, işletmelerin finansal durumunu ya da performansını değerlendirirken kısacası resmin tamamını görmesi açısından son derece önemlidir. Bu durum, muhasebe faaliyetlerinde yapay zekâ uygulamalarını uygun hale getirmektedir. Yapay zekâ, muhasebe ile ilgili olarak birinci veri girişinde insan hatasını ortadan kaldırmaya yardımcı olacak ve bunun sonucu olarak da muhasebe bilgilerinin güvenilirliğini arttıracaktır. Yapay zekâ, denetim faaliyetinde karar verme, örneklem seçimi ve değerlendirme yapılması yönüyle işletmelerde aktif rol oynayacaktır. Denetim sürecinde yapay zekâ uygulamaları verimliliği arttırdığı gibi insan hatasından kaynaklanan hata ya da hilenin önlenmesinde de etkili olacaktır. Özellikle yapay zekâ, zaman alan denetim aşamalarında denetçilere faydalı olacaktır (Zemankova, 2019, s. 149).

Denetim mesleği, teknolojik değişimler nedeniyle zaman içerinde önemli ölçüde değişikliğe uğramıştır. Bu meslekle ilgili olarak birçok değişikliğe şimdiden tanıklık edilmektedir. Bunlar; denetim kurallarının sayısındaki artış, mesleki etik standartlarındaki çok sayıda değişiklik, denetim işinin kalitesinin artması, denetim firmaları arasında artan rekabet ve müşterilere yeni hizmetlerin sağlanması gibi değişiklikleri içermektedir. Bununla birlikte denetçiler, yeni denetim türlerinin ve hizmetlerinin gelişimine tanıklık etmişlerdir. Bu gelişmeler neticesinde denetim mesleği her zamankinden daha da rekabetçi hale gelmiştir. Denetçiler, rakiplerinden üstün olma çabasına bağlı olarak karar verme sürecini hızlandırmak ve kolaylaştırmak için yapay zekâ araç ve yöntemlerini benimsemişlerdir (Al-Sayyed vd., 2021, s. 283).

Denetim, yapay zekâ kullanımı gerektiren mesleklerden biri haline gelmiştir. Dalal (1999, s. 1), *"Dünya nüfusunun hayal edilemez seviyelere ulaşması ve işlemlerin doğasındaki karmaşıklık nedeniyle denetim prosedürlerinin uygulanması neticesinde giderek yazılıma bağımlı hale gelecektir. Yapay zekâ ve uzman sistemler bundan dolayı faydalıdır ve belki de günümüz denetim işlemlerinin yürütülmesinde kaçınılmazdır"* ifadesinde yapay zekânın kullanılmasının öneminden bahsetmiştir. Bu ifadeyi destekleyici olarak son yıllarda denetçilerin karar vermelerine yardımcı olmak için karmaşık yapıya sahip olan yapay zekâ sistemleri daha çok kullanılır hale gelmiştir (Abdolmohammadi ve Usoff, 2001, s. 142). Denetim süreçlerinde yapay zekâ uygulamalarına ilişkin olarak sözleşmelerin gözden geçirilmesi örnek olarak verilebilir. Makine öğrenimi cihazları, denetçilerin daha kısa sürede geleneksel denetim yöntemlerine kıyasla daha fazla sözleşme incelenme olanağı sağlamaktadır (Schmidt vd., 2020, s. 37). Diğer bir ifadeyle akıllı cihazlar, denetçilerin yapabileceğinden daha ileri düzeyde doğrulukla, önceden belirlenen kriterleri kullanarak analiz edebilir ve gerekli bilgileri hızlı bir şekilde sonuç elde etme imkânı sağlamaktadır (Issa ve Varsarhelyi, 2016, s. 4).

Denetim faaliyetinde kullanılacak olan yapay zekâ sisteminin amacı, denetim işlemlerinde manuel olarak karar verme süreçlerinde meydana gelebilecek olası önyargıları ve eksiklikleri dikkate alarak denetçilerin daha doğru karar almasına yardımcı olmaktır. Aslında bu tür yargıların gerekliliği olarak çok yönlü ve hassasiyete bağlı olarak yapay zekâ sistemlerinin denetçinin karar vermesinde yalnızca yardımcı ya da girdi olarak kullanılması gerektiğine inanılsa da ((Abdolmohammadi ve Usoff, 2001, s 147); bazı araştırma sonuçlarına göre ise denetçilerin bu yapay zekâ sistemlerinin sonuçlarına aşırı güvendiğini göstermektedir (Glover vd., 1996, s. 200; Swinney, 1999, s. 202). Aslında denetçinin, yapay zekâ sistemini sadece *"aracı"* olarak kabul etmesi gerekmektedir. Denetim işlevlerini yapay zekâ aracılığıyla sorgulamak hem müşteri hem de işletme için devasa iş yükünü azaltacaktır. Denetçi, muhasebe terimleri ve risk çözme faktörleriyle ilgili yansımaları ve üstün yönleri belirlemek için yapay zekâ sistemleri aracılığıyla kolayca verileri toplayabilir (Gusai, 2019, s. 61). Bu nedenle, yapay zekâ sistemini kullanırken; amacına uygunluğu, güvenilirliği ve etkinliğini sağlamak denetçinin sorumluluğundadır. Aslında denetim de son karar aşamasında yapay zekâ sistemlerinin kullanılması iki ucu keskin bir kılıç gibidir. Denetçi, hatalı olduğu ortaya çıkan bir karar alırken modern sistemi yeterince kullanmamaktan

sorumlu olabileceği gibi; kararını bir uzman sisteme dayandırarak hatalı karar almaktan da sorumlu olabilir (Sutton vd., 1994, s. 201).

Denetimde yapay zekânın kullanılması üç tür denetim riskini azaltmaktadır. Bunlar; yapısal risk, kontrol riski ve tespit riskidir. Bununla birlikte iç denetim süreçlerinde de, teknolojik değişmeler sonucunda stratejik ve operasyonel risklere karşı yapay zekâ sistemi aracılığıyla destek alması gerekmektedir. Bununla birlikte denetim rolü değişirken denetçilerin oynamaları gereken roller ve üstlendikleri riskleri belirlemek için yapay zekânın risklerini ve fırsatlarını iyi anlamaları gerekmektedir. IIA'ya (2017) göre yapay zekâ sistemlerinden kaynaklanan riskler çok çeşitlidir. Bunlar (IIA, 2017);

- Yapay zekâ, insan mantığı sapmalarını ve bilinmeyen eğilimleri benimseyebilir,
- Çeşitli etik ve itibara ilişkin risk sorunları,
- Yapay zekâyı benimsemenin yüksek maliyeti,
- Yapay zekâyı benimsemeyen işletmelerdeki rekabet riskleridir.

Son dönemde denetim süreçlerinde yapay zekâ sistemlerinin kullanılmasının yaygınlaşması sonucunda denetim firmalarının en son teknolojik yeniliklere yatırım yapmasını zorunlu hale getirmiştir (Alles ve Gray, 2019, s. 112). 4 büyük denetim firmasının her biri yapay zekâ sistemlerine yaklaşık olarak 250 milyon dolar harcadığı bilinmektedir (Elliott vd., 2017, s. 52). Aynı zamanda 4 büyük denetim firmalarından biri olan PwC, 2030 yılına kadar yapay zekâya yapılacak yatırımların 15,7 trilyon dolar olacağını tahmin etmektedir (Munoko vd., 2020, s.). Firmaların yüksek fiyat ödemesinin nedeni yapay zekâ sisteminin denetim sürecinin verimliliğini ve etkinliğini artırmasıdır. Ayrıca yapay zekâ; görme, duyma, mantıksal testler yapma, öğrenme ve problem çözme gibi insan davranışlarını taklit edebilmektedir (Li ve Liu, 2020, s. 92).

Yapay zekâ yardımı ile denetçiler, veriler çıkarabilir ve birleştirebilir, bunun sonucu olarak denetim süreçlerinin farklı aşamalarının daha iyi anlaşılmasını sağlayabilirler (Al-Sayyed vd., 2020, s. 283). Bununla birlikte, yapay zekâdan faydalanılarak yapılacak ek denetim görevleri (Baldwin vd., 2006, s. 80);

- Denetim kanıtı elde etmek amacıyla analitik gözden geçirme prosedürleri,
- Sınıflandırma ya da belirli bir muhasebe kaleminin neyi temsil ettiğine karar verme,
- Önemlilik değerlendirmesi yapma,
- Firmanın süreklilik ilkesine ilişkin kararlar, firmanın devamlılığını tehlikede olup olmadığını belirleme,
- İflas tahminidir.

Kısaca denetçilerin, denetim faaliyetlerinde yapay zekâ tabanlı sistemleri kullanmalarının çeşitli faydaları bulunmaktadır. Yukarıdakilere ek olarak bu faydalar; verimlilik ve etkinlik (Abdulmohammadi veUsoff, 2001, s. 175), tutarlılık, gelişmiş, karar verme ve iletişim (Brown ve Murphy, 1990, s. 65), tecrübesiz olanlar için uzmanlık geliştirme ve daha kısa sürede karar verme (Eining ve Dorr, 1991, s. 3) olarak sıralanabilir. Yapay zekâ sisteminin faydaları olduğu kadar dezavantajları da söz konusudur. Bunlar; daha fazla alternatiflerin sonucu olarak uzun süreli karar verme süreçleri (Mackay vd., 1992, s. 651), tecrübesiz personelin bilgi tabanının engellenmesi (Murphy, 1990, s. 21), mesleki muhakeme becerilerini geliştirmenin engellenmesi (Yuthas ve Dillard, 1996, s. 57), araçların rakiplere devredilme riski ve alınan kararla ilgili kanıtlara aşırı güvenildiği için bir mahkeme sürecinde denetçiye kullanma olasılığı (Abdulmohammadi veUsoff, 2001, s. 182) olarak belirtilmiştir.

Yapay zekanın, işletmeler tarafından yaygın bir şekilde kullanılmasında iç denetçilerin rolü kaçınılmazdır. Bu teknolojik gelişmeler karşısında yapay zeka ile ilgili yol haritasının belirlenmesinde iç denetçiler birçok yönüyle fayda sağlayacaktır. Gelecek dönemde işletmelerde iç denetim faaliyetlerinin yürütülmesi noktasında iç denetçinin danışmanlık rolü ön plana çıkarılacaktır (TİDE, 2017, s. 1). Bundan dolayı işletme içerisinde iç denetçi hem denetçi rolüne sahip olması hem de yapay zekanın işletmeler de rahat bir şekilde uygulanması ve geliştirilmesi yönüyle iç denetçi danışmanlık rolünü üstlenecektir. Böyle bir sisteminin içerisinde iç denetçi, denetim ve kontrol algoritmaların hazırlanması, yapay zeka sisteminin aktif hale geldikten sonra denetim performansının takibi ve çıktıların gözden geçirilmesinde aktif rol oynayacaktır (Özcan, 2022). Özellikle borsada işlem gören işletmelerin operasyonlarının çeşitlenmesi ve yapay zeka teknolojisinin hızla gelişmesi karşısında geleneksel denetim yöntemleri işletmelerin iç denetim gereksinimlerini karşılayamayacaktır. İşletmeler kendi işletmelere uygun olan iç denetim standartlarını ve denetim firmalarını formüle etmesi gerekecektir. Bunun sonucunda, işletme tarafından seçilen iç denetim yöntemi de işletmenin gelişim hedefleriyle ve yapay zeka ile uyumlu olması gerekmektedir. İç denetim de yapay zeka yöntemini kullanmalarının işletmelere sağladığı avantajlar; işletmenin gelişimini engelleyen sorunları zamanında tespit edilebilir ve ilgili risk uyarılarını önceden sağlayabilir, işletmenin yönetim kararları için değerli fikirler sağlayabilir, kurumsal yönetimin sürekli

iyileştirilmesini teşvik edebilir. Modern bilim ve teknolojinin gelişmesi, yapay zeka teknolojisinin gelişimini oldukça dikkat çekici hale getirdiğinden yapay zekanın iç denetim üzerindeki etkisi dikkate alınmalıdır (Li vd., 2020, s. 28).

İşletmelere denetim süreçlerinde fayda sağlayan üç tip yapay zekâ türü bulunmaktadır. İlk olarak karar verme süreçlerinde bireylere yardımcı olan ya da insanların hali hazırda yapmakta olduğu birçok görevi yenileyerek farklı durumlara tepki veren *"destekli yapay zekâ sistemleri"* olarak bilinen sistem söylenebilir. Bu sisteme göre makineler, işlemleri yapıyor ve denetçiler bunun neticesinde karar veriyorlar. Bu sistem, yapay zekânın günlük görevlerini yerine getirmesine izin verdiğinden dolayı *"mekanik zekâ"* olarak tanımlanmaktadır (Munoko vd., 2020, s. 8). İkincisi makinenin karar verme sürecinde insanla işbirlikçi olması gerektiren *"artırılmış yapay zekâ sistemi"'dir*. Bu sistemler, çevreleriyle etkileşime girebildiği ve denetçiden bilgi öğrenebildiği için bu sistem *"analitik zekâ"* olarak kabul edilmektedir (BAI, 2017, s. 246). Bu sistemde, denetçiler ve yapay zekâ sistemi ortak karar vericidir. Bununla birlikte firmaların daha önce ulaşılamayan hedeflere ulaşmasını sağlamaktadır. Üçüncü olarak ise çeşitli koşullara uyum sağlayabilen ve denetçi müdahalesi olmadan hareket edebilen *"otonom yapay zekâ sistemi"* dir. Bu sistem sürecinde denetçi, karar vermeyi yapay zekâya aktarmaktadır. Otonom sistem hem *"sezgisel"* hem de *"empatik"* zekâ göstermektedir. Sezgisel zekâ, yapay zekânın yeni durumlara yenilikçi ve etkili şekilde değişiklik yapmasını sağlar. Empatik zekâ ise yapay zekânın bireysel duyguları tanımasına ve bireyleri etkilemesine olanak tanımaktadır (Munoko vd., 2020, s. 12). Bu sistemlerin denetim süreçlerinde uygulanması, daha yüksek kalitede denetim kararlarının alınmasında etkili olmaktadır.

3. UYGULAMA

Uygulama başlığı altında araştırmanın konusu ve amacı, kapsamı, sınırlılıkları ve sayıltıları, evren ve örneklemi, yöntemi, hipotezleri, araştırma ölçeğinin güvenilirliği ile araştırmada elde edilen verilerin analiz sonuçları yer almaktadır.

3.1. Araştırmanın Konusu ve Amacı

Yapay zekâ, başta sağlık olmak üzere iş dünyasının birçok alanında kullanılmakta ve gün geçtikçe kullanımı yaygınlaşmaktadır. Bu açıdan bakıldığında yapay zekâ sistemlerinin muhasebe ve finans alanında da kullanımı mümkün müdür? Denetim alanında kullanımı söz konusu olabilir mi? Denetçiler yapay zekâyı kolaylıkla faaliyetlerinde kullanabilirler mi? Kullanırlarsa uygulamalarında faydalı olur mu? gibi sorular araştırmanın başlangıcı ve araştırmanın konusunu oluşturmuştur. Bu problematik ile ortaya çıkan konu doğrultusunda, bağımsız denetçilerin yapay zekânın kullanım kolaylığı, kullanımları sonrasındaki fayda beklentileri ile yapay zekânın denetim kalitesine etkisine yönelik beklentilerinin tespit edilmesi amaçlanmıştır. Ayrıca araştırmada, yapay zekânın kullanımı sonrasında ortaya çıkma beklentinin denetim kalitesini etkileme durumu da araştırılacaktır.

3.2. Araştırmanın Kapsam, Sınırlılık ve Sayıltıları

Araştırmanın konu açısından kapsamı sadece yapay zekâ ve denetim ilişkisi olarak belirlenmiştir. Araştırma verileri 2022 yılının ocak ayında toplandığı için zaman sınırını bu tarih belirlemiştir. Ayrıca araştırma verileri Antalya, Isparta ve Burdur illerinde faaliyet gösteren bağımsız denetçilerden elde edildiği için bu yerleşim birimleri araştırmanın yer sınırını oluşturmaktadır. Belirtilen konu, zaman ve yer bakımından ortaya konulan hususlar, araştırmanın dışında bırakılmıştır.
Araştırmanın birinci sayıltısı, araştırma katılımcıları soruları tam olarak anlamışlar ve araştırmanın amacı kapsamında yanıtlamışlardır. İkinci sayıltısı, araştırma, verilerin elde edildiği zaman, konu ve yer sınırlılıkları dahilinde geçerlidir. Üçüncü sayıltısı, örneklem olarak belirlenen grup, evreni temsil etme yeteneğine sahiptir.

3.3. Araştırmanın Evren ve Örneklemi

Araştırmanın evreni Antalya, Isparta ve Burdur'da faaliyet gösteren bağımsız denetçilerdir. Bu illerde toplam 629 denetçi bulunmaktadır (www.KGK.gov.tr). Araştırma kapsamı dahilinde 251 bağımsız denetçiye ulaşılmış ve yüz yüze anket uygulaması gerçekleştirilmiştir.

3.4. Araştırmanın Hipotezleri

Gelişen yeni teknolojileri tanıtmak ya da pazara sunmak hedef kitle tarafından kullanılmadığı sürece yenilik olarak kabul edilmeyecektir (Mlekus vd., 2020). Öncelikle hedef kitlenin yeni teknolojileri kabul etmeleri için bu teknolojinin yaptıkları işi kolaylaştıracağına ve kalitenin iyileşeceğini kabul etmeleri gerekmektedir (Stancheva-Todorova, 2018). Bu değişen dünya karşısında kurum ve kuruluşların rekabet avantajı elde edebilmeleri için yeni teknolojileri yakından takip etmeler ve uygulamaları gerekmektedir. Aynı zamanda kuruluşlar, çalışanlarında yeni teknolojiyi kullanmanın kolaylığını ve kullanışlılığını nasıl algıladıklarını bilmesi gerekmektedir. Ancak bu şekilde çalışanlarını uyumlu olacak şekilde yeni sisteme göre çalışma koşullarını düzenlemeleri gerekmektedir (Mlekus vd., 2020). Bu doğrultuda, denetçinin de yapay zeka ile ilgili algılanan kullanım kolaylığı ve kullanışlılığını tahmin etmek için teknoloji kabul modelinin yaygın olarak kullanılmaktadır (Janvrin vd., 2008). Davis (1989) yeni teknolojinin kabulünü sağlayan iki önemli unsur olduğunu vurgulamıştır. Bunlar; kullanıcıların yeni teknolojiyi benimsemeleri için sistemi kolay, basit ve kullanıcı dostu olarak algılamaları gerekmektedir. Diğeri ise kullanıcının bu sistemi kullanmasının kaliteyi ve iş performansını arttıracağı algıdır. Buna göre yeni bir teknolojik sistemin kullanabilmesi için kullanıcılarda yarattığı algının önemi ortaya çıkmaktadır. Kısacası yeni sistemin uygulanmasında kullanıcının inançları ve tutumları önemlidir. Bu kapsamda araştırmanın konu ve amacı doğrultusunda oluşturulan hipotezler şu şekildedir;

Denetim kalitesi, denetçinin finansal tablolardaki önemli yanlışlıkları belirleme yeteneği; denetçinin denetim sonucunu tarafsız bir şekilde raporunu ifşa etmesi olarak tanımlanmaktadır (Suseno, 2013). Yu (2011), denetim kalitesini uygun kanıtlara dayalı olarak görüş veren, uzman bağımsız denetçi tarafından gerçekleştirilen denetim olarak ifade etmiştir. Denetim kalitesi, denetçiler için son derece önemlidir; denetçilerin tarafsızlığını yansıtır ve denetim görevlerini yöneten denetim standartlarının temel taşı olarak kabul edilmektedir (Fanani vd., 2020). Finansal tabloların denetiminde yapay zeka sisteminin kullanılması denetim kalitesini etkileyecektir. Bu kapsamda araştırmanın konu ve amacı doğrultusunda oluşturulan hipotez şu şekildedir;

H_1: Denetim faaliyetlerinde yapay zekânın kullanımı denetimin kalitesini arttıracaktır.

Yapay zeka sistemi, denetçiler tarafından geniş çapta benimsenmiştir. Denetim faaliyetlerinde yapay zekanın kullanılması, denetçinin karar verme sürecini kolaylaştırmak ve hızlandırmak için zamanında bilgi sağlamaktadır. Yapay zeka sisteminin kullanım kolaylığı; önemli yanlış beyanların tespit etme sürecini geliştirir, manuel inceleme ile uzun sürede yapılacak denetim süreçlerini kısa sürede hassas bir şekilde analiz ederek bilgileri raporlama imkanı sunmaktadır. Kısacası yapay zeka kullanımı denetimin verimliliğini ve kalitesini iyileştirebilir (Zhang vd., 2015). Bu doğrultuda oluşturulan hipotez şu şekildedir;

H_2: Denetim faaliyetlerinde yapay zekânın kullanımın kolaylığı denetiminin kalitesini arttıracaktır.

Yapay zekanın, denetimde kullanılması büyük verilerin daha hızlı şekilde denetlenmesi yönüyle fayda sağlayacaktır. Yapay zeka sistemlerinin kullanılması denetimin etkinliğini arttırmanın yanı sıra denetim verimliliğini önemli ölçüde artıracaktır (Vasarhelyi vd., 2010). Ayrıca yapay zeka sistemlerinin denetim faaliyetlerinde kullanılması, büyük verilerden tahmin modelleri ve davranışsal standartlar oluşturarak denetim sürecinin farklı aşamalarının daha iyi anlaşılmasını sağlayacaktır (Al-Sayyeda vd., 2021). Artık gelişen yapay zeka sistemleri insan müdahalesi olmadan çalışarak, yeni durumlara başa çıkmak için sezgisel zeka ve yapay zekanın bireylere başarılı bir şekilde etkileşime girmesine izin vererek empatik zeka gerekmektedir (Raphael, 2015). Bu doğrultuda oluşturulan hipotez şu şekildedir;

H_3: Denetim faaliyetlerinde yapay zekânın kolaylıkla kullanımı, denetim faaliyetlerinde fayda sağlayacaktır.

3.5. Araştırmanın Yöntemi

Araştırmanın verileri anket uygulaması ile toplanılmıştır. Burdur, Isparta ve Antalya illerinde faaliyet gösteren bağımsız denetçiler bizzat ziyaret edilmiş ve belirlenen sayıya tesadüfi örneklem yöntemi ile ulaşılmıştır.

Araştırmada kullanılan anket, tanımlayıcı ifadeler ve konunun hipotezlerini test etmeye yönelik belirlenen ifadelerden olmak üzere iki kısımda incelenmiştir. Anket hazırlanırken Albawwat ve Al Frijat'in (2021) kullanmış olduğu anket formundan faydalanılmıştır.

Araştırmada elde edilen veriler, SPSS 20 paket programı vasıtasıyla analiz edilmiştir. Öncelikle toplanan veriler güvenilirlik analizine tabi tutulmuştur. Güvenilirliği yüksek derecede güvenilir olduğu için tanıtıcı verilerin frekans ve yüzde dağılımları alınmış ve hipotezlerin kabul/red durumu araştırılmıştır. Hipotezler regresyon yöntemi kullanılarak analiz edilmiştir.

3.6. Araştırma Verilerinin Güvenilirliği

Araştırma anketinden elde edilen verilerin ikinci kısmında yer alan soruların ilk 6'sı yapay zekânın kullanım kolaylığı için katılımcıların algılarını araştıran sorulardan oluşmaktadır. Anketin ikinci kısmında devam eden 6 soru ise yapay zekânın kullanımının faydasına yönelik ortaya çıkması beklenen algıları anlamaya yöneliktir. İkinci kısmın son 11 sorusu ise denetim kalitesine yönelik algıları araştıran sorulardan oluşmaktadır. Bu sorular hem ayrı ayrı hem de toplu olarak güvenilirlik testine tabi tutulmuştur. Bunun sonucunda tablo 1'de yer alan sonuçlara ulaşılmıştır.

Tablo 1. Araştırma Verilerinin Güvenilirliği

	N of Items	Cronbach's Alpha
Birinci Kısım	6	0,977
İkinci Kısım	6	0,990
Üçüncü Kısım	11	0,989
Toplam	23	0,989

Yukarıdaki Tablo 1'den anlaşılacağı $0,80>\alpha>1$ olduğu için üzere araştırmada kullanılan verilerin güvenilirliği, yüksek derecede güvenilirdir. (Kalaycı, 2018: 405).

3.7. Araştırmanın Bulguları

Araştırma bulguları başlığında öncelikle, anket verilerinden elde edilen tanımlayıcı soruların frekans ve yüzde dağılımları, sonrasında ise araştırmanın fonksiyonel verilerinin t testi ve Anova analiz sonuçları yer almaktadır.

3.7.1. Araştırmanın Tanımlayıcı Verilerinin Bulguları

Araştırmanın tanımlayıcı soruları, katılımcılar hakkında bilgi elde etmeye yönelik hazırlanan katılımcıların cinsiyeti, yaşı, eğitim durumu ve mesleki tecrübeleri hakkında bilgi edinmeyi amaçlamaktadır. Katılımcılarla ilgili tanımlayıcı soruların frekans ve yüzde dağılımları aşağıdaki tablo 2'de gösterilmiştir.

Tablo 2. Tanımlayıcı Soruların Frekans ve Yüzde Dağılımları

Tanımlayıcı Sorular	Seçenekler	Frekans	Yüzde
Cinsiyet	Kadın	19	0,08
	Erkek	232	0,92
	Toplam	**251**	**100**
Yaş	25 Yaş ve Altı	38	15,1
	26-35 Yaş Aralığı	46	18,3
	36-45 Yaş Aralığı	78	31,1
	46-55 Yaş Aralığı	23	9,2
	56 Yaş ve Üzeri	66	26,3
	Toplam	**251**	**100,0**
Eğitim Durumu	Lisans	171	68,1
	Lisansüstü	80	31,9
	Toplam	**251**	**100**
Mesleki Tecrübe	5 Yıl ve Altı	86	34,3
	6-10 Yıl Aralığı	85	33,9
	11-15 Yıl Aralığı	26	10,4
	16 Yıl ve üzeri	54	21,5
	Toplam	**251**	**100,0**

Yukarıdaki Tablo 2'de, araştırmanın örneklemini oluşturan Burdur, Isparta ve Antalya illerinde faaliyet gösteren bağımsız denetçilerin tanımlayıcı değişkenlerinin frekans ve yüzde dağılımları gösterilmektedir. Bu tanımlayıcı değişkenlerin birincisini denetçilerin cinsiyetleri oluşturmaktadır. Toplam 251 denetçinin 19'u %08'ini kadınlar oluştururken, geriye kalan 232'sini yani %92'sini erkek katılımcılar oluşturmaktadır. Katılımcıların yaş dağılımları incelendiğinde, 25 yaş ve altı katılımcı sayısı 38 (%15,1), 26-35 yaş aralığı katılımcı sayısı 46 (%18,3), 36-45 yaş aralığı katılımcı sayısı 78 (%31,1), 46-55 yaş aralığı 23 (%9,2) ve 56 yaş ve üzeri katılımcıların sayısı ise 66 (%26,3) olmuştur. Bir diğer değişken olan katılımcıların eğitim durumları incelendiğinde 171 (%68,1) katılımcı lisans, 80 (%31,9) katılımcının lisansüstü mezuniyetine sahip olduğu anlaşılmaktadır. Katılımcıların mesleki tecrübe değişkeni incelendiğinde ise, 5 yıl ve altı tecrübeye 86 (%34,3) denetçinin, 6-10 yıl aralığında tecrübeye sahip 85 (%33,9) denetçi, 11-15 yıl aralığında tecrübeye sahip 26 (%10,4) denetçi, 16 yıl ve üzeri tecrübeye sahip 54 (%21,5) denetçinin çalışmaya dahil olduğu ortaya çıkmaktadır.

3.7.2. Fonksiyonel Değişkenlere İlişkin Bulgular

Bu başlık altında katılımcıların ifadelere verdikleri yanıtlardan elde edilen veriler ile hipotezlerin kabul/red durumları araştırılacaktır.

Aşağıdaki tablo 3'te *denetim faaliyetlerinde yapay zekâ kullanımı ile muhasebe denetiminin kalitesi* arasındaki ilişkiye ilişkin regresyon sonuçları gösterilmektedir.

Tablo 3. Denetim Faaliyetlerinde Yapay Zekânın Kullanımı ile Muhasebe Denetiminin Kalitesi İlişkisi

	R Square	Durbin-Watson	VIF	B	Sig.
Regresion	0,885	2,410	1,000	0,822	0,000
				F	
				895,183	

Yukarıdaki Tablo 3'e göre, oluşturulan model; F=895,183; sig=0,000, 0,05 anlamlılık düzeyinde bir bütün olarak her düzeyde anlamlıdır. Muhasebe denetiminde kalitenin, yüzde 88,5'lik kısmı, yapay zekânın denetim faaliyetlerinde kullanımı ile açıklanmaktadır (Kalaycı, 2009: 203). Yapılan regresyon analizi ile denetim faaliyetlerinde yapay zekânın kullanımındaki 1 birimlik artış, muhasebe denetimindeki kaliteyi 0,822 birim artırmaktadır. Yapılan analizde elde edilen Durbin Watson değerinin 2,410 olması yine modelde otokoreslasyon olmadığını göstermektedir. Bunun yanında 1,000'lık VIF değeri, bağımsız değişkenler arasında çoklu bağlantı olduğunu göstermektedir. Yapılan bu analizler sonucuna göre **H_1 hipotezi kabul** edilmiştir. Bu sonuca göre, denetçilerin yapay zeka sistemini kullanmalarının denetim kalitesine önemli ölçüde arttırdığını algıladıklarının göstergesidir.

Aşağıdaki tablo 4'te *denetim faaliyetlerinde yapay zekânın kullanımının kolay olması ile muhasebe denetiminin kalitesi* arasındaki ilişkiye ilişkin regresyon sonuçları gösterilmektedir.

Tablo 4. Denetim Faaliyetlerinde Yapay Zekânın Kullanımının Kolay Olması ile Muhasebe Denetiminin Kalitesi İlişkisi

	R Square	Durbin-Watson	VIF	B	Sig.
Regresion	0,612	1,959	1,000	0,831 **F** 393,364	0,000

Yukarıdaki tablo 4'e göre, H_2 hipotezi ile denetçilerin denetim faaliyetlerinde, yapay zekâyı kolaylıkla kullanabilmelerinin, denetim sürecinde kaliteyi etkileyip/etkilemeyeceğinin araştırıldığı anketlerin analizleri sonucunda oluşturulan model 0,05 anlamlılık düzeyinde bir bütün olarak anlamlıdır. R^2=0,612 değeri denetim faaliyetlerinde kalitenin etkilendiği unsurlar içerisinde yüzde 61,2'lik kısmının yapay zekânın kullanım kolaylığı tarafından açıklanmaktadır. Durbin-Watson testi sonucunda tablo 4'teki modelde katsayı 1,5-2,5 aralığında olduğu için otokorelasyon olmadığı görülmektedir. Regresyon analizi sonucunda muhasebe denetiminde yapay zekânın kullanımının kolaylaşmasının 1 birimlik artışı, muhasebe denetiminin kalitesinin 0,831 birim arttırmaktadır. Ayrıca modelde bağımsız değişkenler arasında çoklu bağlantı olduğu da görülmektedir. Elde edilen bütün bu sonuçlardan dolayısıyla **H_2 hipotezi kabul** edilmektedir. Buna göre, yapay zekâ sistemleri manuel incelemelerini yapabileceğinden daha ileri düzeyde daha önceden belirlenen kriterlerle kolay bir şekilde denetimi gerçekleştireceği ve kolaylıkla hata ya da hilelerin ortaya çıkartabilecektir. Bununla birlikte yapay zekâ sistemlerinin denetçiler tarafından kabul etmesi için kullanım kolaylığı esastır.

Aşağıdaki tablo 5'te *denetim faaliyetlerinde yapay zekânın kullanımının kolay olması ile muhasebe denetim faaliyetlerinde fayda sağlaması* arasındaki ilişkiye ilişkin regresyon sonuçları gösterilmektedir.

Tablo 5. Denetim Faaliyetlerinde Yapay Zekânın Kullanımının Kolay Olması ile Muhasebe Denetim Faaliyetlerinde Fayda Sağlaması İlişkisi

	R Square	Durbin-Watson	VIF	B	Sig.
Regresion	0,765	1,470	1,000	0,875 **F** 352,069	0,000

Yukarıdaki Tablo 5'te, H_3 hipotezine yapılan regresyon analizi sonuçları yer almaktadır. Analiz sonuçlarına göre oluşturulan modelin F değeri 352,069; sig değeri ise 0,000<0,05 olduğu için hipotez kapsamında oluşturulan model istatistiksel açıdan bir bütün olarak anlamlıdır. Dolayısıyla oluşturulan **H_3 hipotezi kabul** edilmiştir. Araştırma kapsamında ulaşılan denetçilerin, muhasebe denetim faaliyetlerinde yapay zekânın kullanımının %76,5'lık kısmı yapay zekâ kullanım kolaylığı tarafından açıklanmaktadır. Yapılan analiz sonucunda denetçilerin, denetim faaliyetlerinde yapay zekânın kullanım kolaylığına yönelik düşüncelerindeki 1 birimlik artış, yapay zekâyı muhasebe denetim faaliyetlerinde kullanımını 0,875 birim arttırmaktadır. Ayrıca modelde DW=1,570 değeri otokorelasyon olmadığını ve 1,000'lık VIF değeri bağımsız değişkenler arasında çoklu bağlantı olduğunu göstermektedir. Denetim faaliyetlerinde yapay zeka sisteminin sonuçlarına denetçiler tarafından aşırı güvenildiğini bu yönüyle de denetçilerin daha hızlı ve iyi kararlar almasına yardımcı olduğu söylenebilir.

4. SONUÇ VE ÖNERİLER

Denetim görevleri çok sayıda işlem gerektirdiği için kapsamlı ve karmaşık bir yapıya sahiptir. Denetçilerin denetim faaliyeti kapsamında karşılaştıkları denetim sorunlarına daha eksiksiz ve kaliteli çözümler bulanabilmesi açısından yapay zekâ sistemleri uygulamalarını kullanmak yadsınamaz bir gerçeklik olarak karşımıza çıkmaktadır. Son yıllarda kullanımı oldukça artan yapay zekâ sistemleri, denetim sürecini önemli ölçüde değiştirmiştir. Ancak, sınırlı sayıda araştırmada denetçilerin yapay zekâ uygulamalarının kolaylığı, kullanım kolaylığı ve faydasına ilişkin algıları incelenmiştir.

Bu araştırmada, Antalya, Isparta ve Burdur illerinde faaliyet gösteren 251 bağımsız denetçiye yapay zekânın kullanım kolaylığı, kullanımları sonrasındaki fayda beklentileri ile yapay zekânın denetim kalitesine etkisine yönelik beklentilerinin tespit etmek için online anket uygulanmıştır. Ayrıca araştırmada, yapay zekânın kullanımı sonrasında ortaya çıkma beklentisinin denetim kalitesini etkileme durumu da araştırılmıştır. Araştırma verilerine ilk olarak güvenilirlik testi yapılmış ve soruların güvenilirliği ile ilgili olarak yüksek derecede güvenilir olduğu tespit edilmiştir. Sonrasında ankete katılanların frekans ve yüzdelik dağılımlarına ilişkin bilgilere ulaşılmış ve metin içerisinde detayları verilmiştir. Araştırmada, oluşturulan 3 adet hipotez ise regresyon yöntemi ile analiz edilmiştir.

Yapılan analiz sonucunda, oluşturulan 3 adet hipotez de kabul edilmiştir. Elde edilen analiz sonucuna göre; denetim faaliyetlerinde yapay zekâ kullanımının denetim kalitesini arttıracağını, denetim faaliyetlerinde yapay zekâ kullanımı kolaylığının denetiminin kalitesini arttıracağı ve denetim faaliyetlerinde yapay zekânın kolaylıkla kullanımının, denetim

faaliyetlerinde fayda sağlayacağı saptanmıştır. Daha önceki araştırmalarda yapay zekânın denetim faaliyetlerinde kullanmanın faydalarını; müşterilerin riskler hakkında daha iyi anlayış oluşmasına, yanlış beyanların tespit edilmesinde ve yöneticilerle iletişimin gelişmesinde etkili olduğu saptanmıştır. Aynı zamanda yapay zekâ sistemlerinin benimserken denetçilerin bu sistemleri kabul etmesinin ön şartı kullanım kolaylığıdır. Denetçilerin yapay zekâ sistemlerini kolay bir şekilde uygulamaları denetim sürecinde insan hatasının ortadan kaldırılmasına ve bu durumda muhasebe bilgilerinin güvenilirliğinin artmasını etkileyecektir.

Bu araştırmada, sadece belirli bölgede faaliyet gösteren bağımsız denetçilerden elde edilen veriler kullanılmıştır. Bu araştırmanın sonuçlarını genelleştirebilmek için Türkiye'de faaliyet gösteren tüm denetçilere ya da diğer ülkelerdeki denetçilere aynı anket soruları uygulanıp, elde edilen sonuçlar karşılaştırılabilir. Gelecekteki araştırmalarda, denetçilerin yapay zekâ sistemlerini kullanım kolaylığı ya da algılanan faydayı ölçmek için denetçilere eğitim verilerek test edilebilir. Aynı zamanda yapay zekâ sistemlerinin iş kalitesine etkisini değerlendirmek amacıyla diğer meslek gruplarına da anket soruları uygulanabilir.

Ek: Anket Forum

Bölüm 1: Denetçilerin Yapay Zekâya Yönelik Algılarının Analizi Ve Denetim Kalitesine Katkısı

	Kesinlikle Katılmıyorum	Katılmıyorum	Fikrim Yok	Katılıyorum	Kesinlikle Katılıyorum
Yapay Zekâ'nın Kullanım Kolaylığı için Algılanan Öğeler					
Yapay zekâ sistemlerini ve araçlarını denetimde kullanmayı öğrenmek benim için kolay olurdu.					
Yapay zekâ sistemleri ve araçları ile denetimde yapmak istediklerimi kolay şekilde bulurum.					
Denetimde yapay zekâ sistemleri ve araçlarıyla etkileşimim açık / anlaşılır olacaktır.					
Denetimde yapay zekâ sistemlerini ve araçlarını etkileşim açısından esnek bulabilirim.					
Denetimde yapay zekâ sistemleri ve araçları konusunda uzmanlaşmak benim için kolay olurdu.					
Denetimde yapay zekâ sistemlerini ve araçlarının kullanımı kolay olacaktır.					
Yapay Zekâ'nın Kullanışlılığı ile ilgili Algılanan Öğeler					
Gelecekte, denetim işimde yapay zekâ sistemlerini ve araçlarını kullanmak, görevleri daha hızlı tamamlamamı sağlayacaktır.					
Gelecekte, denetim işinde yapay zekâ sistemlerini ve araçlarını kullanmak, iş performansımı iyileştirecektir.					
Gelecekte, yapay zekâ sistemlerini ve araçlarını kullanmak, denetim işimde üretkenliğimi artıracaktır.					
Yapay zekâ sistemlerini ve araçlarını kullanmak, denetim işimin etkinliğini artıracaktır.					
Gelecekte, yapay zekâ sistemlerini ve araçlarını kullanmak, denetim işimi yapmamı kolaylaştıracaktır.					
Gelecekte, denetim işimde yapay zekâ sistemlerini ve araçlarını faydalı bulabilirim.					
Denetim Kalitesine Etki Eden Öğeler					
Denetimde yapay zekâ sistemlerini ve araçlarını kullanmak, mesleki şüpheciliğime yardımcı olacaktır.					
Denetimde yapay zekâ sistemleri ve araçlarının kullanılması, rutin denetim süreçlerini ve prosedürlerini otomatikleştirerek, önemli yargı alanlarına odaklanmak için daha fazla zaman sağlar.					
Denetimde yapay zekâ sistemlerini ve araçlarını kullanmak, kurum ve süreçleri hakkındaki anlayışımı derinleştirecektir.					
Denetimde yapay zekâ sistemlerinin ve araçlarının kullanılması, tüm popülasyonların analizi yoluyla sağlam risk değerlendirmesini kolaylaştıracaktır.					
Denetimde yapay zekâ sistemlerinin ve araçlarının kullanılması, denetim süreci boyunca devam eden risk değerlendirmesine olanak sağlayacaktır.					
Denetimde yapay zekâ sistemleri ve araçlarının kullanılması, büyük popülasyonların katmanlandırılması yoluyla denetim testinin en yüksek risk altındaki alanlara odaklanmasını kolaylaştıracaktır.					
Denetimde yapay zekâ sistemlerini ve araçlarını kullanmak, manuel yaklaşımın mümkün olmadığı büyük veya karmaşık veri kümeleri üzerinde testler yapmamı sağlayacaktır.					
Denetimde yapay zekâ sistemleri ve araçlarının kullanılması, karmaşık hesaplamaların ve modellemenin bağımsız olarak yeniden gerçekleştirilmesini sağlayacaktır.					
Denetimde yapay zekâ sistemleri ve araçlarının kullanılması, grup denetimlerinde tutarlılığı ve merkezi gözetimi iyileştirecektir.					
Denetimde yapay zekâ sistemleri ve araçlarının kullanılması ile olası hile tespit edilebilecektir.					
Denetimde yapay zekâ sistemlerinin ve araçlarının kullanılması, daha geleneksel denetim teknikleri kullanılarak fark edilemeyebilecek olağandışı kalıpları ve istisnaları belirleyecektir.					

Bölüm 2: Kişisel Bilgiler

Cinsiyetiniz	Kadın Erkek
Yaşınız:	<25 25-35 36-45 46-55 >55
Eğitim Durumunuz:	Lise: Önlisans: Lisans: Lisansüstü**:**
Mesleki Tecrübe:	1-5: 5-10 10-15 >15
Çalışma Şekliniz:	Bağımsız Denetçi İç Denetçi

Kaynakça

Abdolmohammadi M. J. (1987). Decision support and expert systems in auditing: a review and research directions. *Accounting Business Research Wolters Kluwer UK, 17*(66), 173–185.

Al-Sayyed, S., Al-Aroud, S. F., & Zayed, L. M. (2020). The effect of artificial intelligence on audit evidence. *Accounting, 7*, 281-288.

Albawwat, I., & Frijat, Y. A. (2021). An analysis of auditors' perceptions towards artificial intelligence and its contribution to audit quality. *Accounting, 7*, 755-762.

Alles, M. G., & Gray, G. L. (2020). Will the medium become the message? A framework for understanding the coming automation of the audit process. *Journal of Information Systems, 34*(2), 109-130.

Alina, C. M., Ceresale, S. M., & Gabriela, G. (2018). Internal audit role in artificial intelligence. *"Ovidius" University Annals, Economic Sciences Series, XVII*(1), 441-445.

BAI, G. H. (2017). Research on the application and influence of auditing artificial intelligence. *International Conference on Education Innovation and Economic Management, (ss. 245-249).*

Baldwin, A. A., Brown, C. E., & Trinkle, B. S. (2006). Opportunities for artificial intelligence development in the accounting domain: the case for auditing. *Intell. Syst. Accounting Finance Management, 14*(3), 77–86.

Borthwick, A. F., & West, O. D. (1987). Expert systems--a new tool for the professional. *accounting. Horizon, 1*(1), 9–16, Mar.

Brown, C. E., & Murphy, D. S. (1990). The use of auditing expert systems in public accounting. *Journal of Information Systems*, 63–72.

Byrnes, P. E., Al-Awadhi, A., Gullvist, B., Brown-Liburd, H., Teeter, R., Warren, J. D., Jr., & Vasarhelyi, M. (2012). Evolution of Auditing: From The Traditional Approach To The Future Audit. AICPA White Paper. https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/whitepaper-evolution-of-auditing.pdf Presiden alındı.

Dai, J., & Vasarhelyi, M.A. (2016). Imagineering audit 4.0. *Journal of Emerging Technologies in Accounting, 13*(1), 1-15.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of ınformation technology. *MIS Quarterly, 13*(3), 319-340.

Eining, M. M., & Dorr, P. B. (1991). The impact of expert system usage on experiential learning in an auditing setting. *Journal of Information Systems*, 1–16.

Elliot, V. H., Paananen, M., & Staron, M. (2020). Artificial intelligence for decision-makers. *Journal of Emerging Technologies in Accounting, 17*(1), 51-55.

Etzioni, A., & Etzioni, O. (2017). Should Artificial Intelligence be Regulated?. *Issues In Science & Technology, 33*(4), 32-36.

Fanani, Z., Budi, V., & Utama, A. (2020). Specialist tenure of audit partner and audit quality. *Accounting, 7*(3), 573-580.

Gillett, P., & Vasarhelyi, M A. (1993). Automated dynamic audit programme tailoring: an expert system approach; discussion. *Auditing, 12.*

Gusai, O. P. (2019). Robot human ınteraction: role of artificial ıntelligence ın accounting and auditing. *Indian Journal of Accounting (IJA), 51*(1), 59-82.

Heye, A. M. (2021). The Future of Auditing: An Analysis of AI Implementation in the Big Four Accounting Firms. Honors Theses and Capstones. https://scholars.unh.edu/honors/563 adresinden alındı.

IIA, (2017*). Global Perspectives and Insights, Artificial Intelligence – Considerations for the Profession of Internal Auditing.* Special Edition, Part 1.

Issa, H., Sun, T., & Vasarhelyi, M. A. (2016). Research ideas for artificial ıntelligence in auditing: the formalization of audit and workforce supplementation. *Journal of Emerging Technologies in Accounting, 13*(2), 1-20.

Kalaycı, Ş. (2018*). SPSS Uygulamalı Çok Değişkenli İstatistik Teknikleri* (9. Baskı). Ankara: Asil Yayın Dağıtım.

Li, Q., & Liu, J. (2020). Development of an intelligent nlp-based audit plan knowledge discovery system. *Journal of Emerging Technologies in Accounting, 17*(1), 89-97.

Li, E., Xu, H., & Li, G. (2020). Analysis on improvement of internal audit in china's listed companies based on artificial intelligence. *Advances in Economics, Business and Management Research, 133,* 25-30.

Mackay, J., Barr, S., & Kletke, M. (1992). An empirical investigation of the effects of decision aids on problem-solving processes. *Decision Sciences, 23*, 648–672.

Mlekus, L., Bentler, D., Paruzel, A., Kato-Beiderwieden, A. L., & Maier, G. W. (2020). How to raise technology acceptance: user experience characteristics as technology-inherent determinants. *Gruppe. Interaktion. Organisation. Zeitschrift für Angewandte Organisationspsychologie (GIO), 51*(3), 273-283.

Murphy, D. (1990). expert systems use and the development of expertise in auditing: a preliminary investigation. *Journal of Information Systems*, 18–35.

Omoteso, K. (2012). The application of artificial intelligence in auditing: looking back to the future. *Expert Systems with Applications, 39*(9), 8490-8495.

Özcan, B.D. (2022). Yapay Zekâ Teknolojileri ile İç Denetim Fonksiyonunun ve İç Kontrol Mekanizmalarının İlişkisi. https://medium.com/databulls/yapay-zek%C3%A2teknolojileri-ile-i%CC%87%C3%A7-denetim-fonksiyonunun-ve-i%CC%87%C3%A7-kontrol-mekanizmalar%C4%B1n%C4%B1n-i%CC%87li%C5%9Fkisi-c29240c109a8 adresinden alındı.

Raphael, J. (2015). How artificial intelligence can boost audit quality. CFO Magazine (CFO. com), June, 15.

Schmidt, P. J., Church, K. S., & Riley, J. (2020). Clinging to excel as a security blanket: investigating accountants' resistance to emerging data analytics technology. *Journal of Emerging Technologies in Accounting, 17*(1), 33-39.

Sutton, S. G., Young, R., & McKenzie, P. (1994). An analysis of potential legal liability incurred through audit expert systems. *Intelligent Systems in Finance and Management, 4*, 191–204.

Stancheva-Todorova, E. P. (2018). How artificial intelligence is challenging accounting profession. *Journal of International Scientific Publications Economy & Business, 12*, 126-141.

Suseno, N. S. (2013). The influence of ındependence, size of public accountant office toward audit quality and its impact on public accountant office reputation. *International Journal of Scientific & Technology Research, 2*(3), 123-126.

Swinney, L. (1999). Consideration of the social context of auditors' reliance on expert system output during evaluation of loan loss reserves. *International Journal of Intelligent Systems in Accounting, Finance, and Management, 8*, 199–213.

THE INSTITUDE OF INTERNAL AUDITORS (2017). Küresel bakış açıları ve anlayışlar yapay zeka — iç denetim mesleğine ilişkin dikkate alınması gerekenler, AI PART I.

Ukpong, E. G., Udoh, I. I., & Essien, I. T. (2019). Artificial intelligence: opportunities, issues and applications in banking, accounting, and auditing in Nigeria. *Asian Journal of Economics, Business, and Accounting, 10*(1), 1-6.

Vasarhelyi, M., Alles, M., & Williams, K. (2010). Continuous Assurance for the Now Economy. Sydney, Australia: Institute of Chartered Accountants in Australia.

Yu, H.C. (2011). Legal systems and auditor independence. *Review of Accounting Studies, 16*(2), 377.

Yuthas, K., & Dillard, J. (1996). An integrative model of audit expert systems development. *Advances in Accounting Information Systems, 4*, 55–79.

Zemankova, I. A. (2019). Artificial intelligence in audit and accounting: development, current trends, opportunities and threats – literature review. *International Conference on Control, Artificial Intelligence, Robotics & Optimization (ICCAIRO)* (ss. 148-154).

Zhang, X., Zhao, J., & LeCun, Y. (2015). Character-level convolutional networks for text classification. *In Advances in Neural Information Processing Systems, 28*, 649-657.

İnternet Kaynakları

www.KGK.gov.tr. (Erişim Tarihi, 2 Şubat 2022).

HAKEMLİ Denetişim
Ortak Aklın Harmanı
Kamu İç Denetçileri Derneği Meşrutiyet Caddesi Konur Sokak No: 36/6 Kızılay - ANKARA
www.kidder.org.tr/denetisim/ • denetisim@kidder.org.tr
ISSN 1308-8335
Yıl: 13, Sayı: 26, 45-52, 2022

Teorik Makale

MEZENFORMASYON VE DEZENFORMASYON FAALİYETLERİ, SEKTÖREL RİSKLER VE İLETİŞİM TEKNOLOJİLERİ

(MISINFORMATION AND DISINFORMATION ACTIVITIES, SECTORAL RISKS AND COMMUNICATION TECHNOLOGIES)

Dr. Nurat KARA[*],

ÖZ

Bilgi bozukluğu iletişim teknolojilerinin yaygınlaşması ile ulusal ve uluslararası bir sorun olma yolunda ilerlemektedir. Teknolojilerin hızla gelişmesi, yaşanan sosyo-ekonomik olaylar ve küresel sağlık problemleri gibi konular ekseninde bilgi bozukluğu sürekli önemi artan bir konu olarak karşımıza çıkmaktadır. Genellikle mezenformasyon veya dezenformasyon olarak detaylandırılan bilgi bozukluğu toplumları etkilediği gibi kamu ve özel sektörü de etkisi altına almaya başlamıştır. Hem dezenformasyon, yani kasıtlı yanıltma, hem de mezenformasyon, yani farkında olmadan bilgi bozukluğuna sebebiyet verme, toplumları ve sektörleri yeni bir takım siber tehditlerle karşı karşıya bırakmaktadır. Bu durum bazı, yeni ve ciddiye alınması gereken sektörel riskleri de beraberinde getirmektedir. Bazı sektörel risklerle birlikte, yeni iletişim olanaklarının hızla çeşitlenmesi dijitalleşmeyi ve siber tehditleri de yaygınlaştırmaktadır. Dijital dönüşüm bir yandan sektörler için bazı yeni olanakları yaratsa da meydana getireceği muhtemel siber sorunların şimdiden dikkate alınması önemli bir çalışma alanı olarak düşünülmektedir. Aksi durumun ileride önemli birtakım olumsuz sonuçları beraberinde getirmesi olasıdır. Bu çalışma ile bilgi bozukluğunun, hem dezenformasyon hem de mezenformasyon, sektörel olarak yaratacağı riskleri anlamak ve de bu risklere yönelik birtakım önerileri sunmak amaçlanmaktadır. Çalışmada bu öneriler şu şekilde sıralanmıştır: Dijital dönüşüm stratejileri oluşturmak, siber riskleri belirlemek ve değerlendirmek, standartlar ve normlar belirlemek ve benimsemek. Bunun yanı sıra, mezenformasyon ve dezenformasyonu önlemek için çeşitli endüstriler, kamu ve özel sektör, uluslararası liderler ve siyasi liderlere fayda sağlayabilecek ortaklıklarla yatırımları artırmak önem arz etmektedir. İşbirliği içerisinde olacak olan bu aktörler yeni iletişim teknolojilerinin alt yapısına yapacakları yatırımlarla ve kurulacak ortak sistemlerle küresel boyutta dezenformasyon ve mezenformayson ile mücadale edebilirler.

Anahtar Kelimeler: Bilgi Bozukluğu, Sektörel Tehditler, Siber Güvenlik, İletişim Teknolojileri, Dezenformasyon

Jel Kodları: M, O3

ABSTRACT

Information disorder is on its way to becoming a national and international problem with the spread of communication technologies. Information disorder is a constantly increasing issue in the axis of issues such as the rapid development of technologies, socio-economic events, and global health problems. Information disorder, often detailed as misinformation or disinformation, has begun to affect the sectors and societies. Both disinformation, that is, deliberate deception, and misinformation, causing information corruption without being aware of it, expose societies and sectors to a new set of cyber threats. This situation brings some new and sectoral risks that should be taken seriously. Along with some sectoral risks, the rapid diversification of new communication opportunities makes digitalization and cyber threats widespread. Although digital transformation creates some new opportunities for the sectors, it is considered an essential field of study to consider the possible cyber problems it will create. Otherwise, it may bring some essential negative consequences in the future. This study aims to understand the risks that information disorder will create both disinformation and misinformation sectoral and present

• Dr., Bilgi İşlem Daire Başkanı, Hatay Mustafa Kemal Üniversitesi, 0000-0001-9753-1593, nkara@mku.edu.tr

some suggestions for these risks. In the study, these recommendations are listed as follows: Creating digital transformation strategies, identifying, and evaluating cyber risks, setting and adopting standards and norms, preventing misinformation and disinformation, and ***increasing investments with various industries, sectors, and international leaders and partnerships that can benefit leaders.***

Keywords: *Information Distortion, Sectoral Threats, Cyber Security, Communication Technologies, Disinformation*

JEL Classification: *M, O3*

1. GİRİŞ

Yeni bir bilgi çağının içindeyiz; eski teknolojilerin yeni teknolojilere evirildiği ve bilgi teknolojilerine dayanan üçüncü sanayi devriminden sonrasını tecrübe etmekteyiz. Dördüncü sanayi devrimi, pek çok zaten hayatımızda olan teknolojinin olgunlaşması akabinde bir araya gelmesinden meydana gelmektedir. Artan insan kaynakları maliyetleri ve diğer başka sebepler teknoloji tabanlı yeni sistemlerin kurulmasını gerekli kılmıştır. Dolayısıyla ilk üç devrimin ötesinde üretim süreçlerinde insansızlaşmaya gidilen dördüncü sanayi devriminden bahsedilmektedir. Dördüncü sanayi devrimi ile birlikte hem kamu hem de özel sektörlerde, toplumsal bir değişim yaşanmakta ve değişimle birlikte yeni birtakım riskleri de konuşur hale gelmekteyiz (Schwab, 2017). Kaplan ve Haenlein' göre ise (2019, s. 679), dijital dönüşüm, dijital teknolojilerin toplumu tüm alanlarda entegre ederek ve büyük ölçekte değişimlere maruz bırakmaktadır. Bu değişime dijital dönüşüm denilmektedir. Dijital dönüşüm bir yandan toplumları değiştirirken diğer taraftan hükümetleri ve kamu yönetimini de etkisi altına almaktadır (Kaplan ve Haenlein, 2019). Bu dönüşümün küresel olarak her sektöre etkisi bulunmakta ve bu etki değişimi zorunlu kılmaktadır (Schwab, 2017). Hem kamu hem özel sektörün bu değişim sebebi ile çok zorlanacağı bir gerçektir (Saarikko et al., 2020). Dijitalleştirilmiş bilgi, ürün ve hizmetlerin yanı sıra dijital ve fiziksel bileşenleri entegre eden sistemlerin ve sektörlerin ayrılmaz bir parçası haline gelmektedir (Saarikko et al., 2020). Kamu ve özel sektörün kullandığı ve oluşturduğu bilgi ve bu bilgiyi işlemek için kullanılan geniş teknoloji yelpazesi endüstrileri dönüştürebilir, sektörler için rekabet avantajlarını yeniden şekillendirebilir ve yeniliği yönlendirebilir durumdadır (Porter ve Millar, 1985). Kaliteli bilgi edinme, sektörel bazda dönüşüm, performans ve sürdürülebilir olmak yeni mücadele alanları olarak görülmektedir.

Öte yandan bilgi bozukluğu, genellikle, mezenformasyon ve dezenformasyon olarak değerlendirilir. Bu bir süredir önemli bir endişe kaynağı olsa da siber saldırıların sıklığı ve karmaşıklığındaki sürekli artış, seçim sürecinde ortaya çıkan bilgi kirliliği COVID-19 sırasında ortaya çıkan bilgi bozukluğu gibi krizler, bu durumu sektörler için bir soruna dönüştürdü. Bilgi bozukluğu, kuruluşlar için önemli tehditler ve riskler oluşturur. Dünya Ekonomik Forumu'nun 2013 Küresel Risk Raporu, dijital bilgi bozukluğu riskinin altını çizmektedir. Dijital dezenformasyon riski daha sonra 2016 ABD başkanlık seçimlerinde ve COVID-19 krizi boyunca geniş çapta tanındı. Bu vakalarda bilgi bozukluğunun etkisi önemli olmuştur. Bu bağlamda çalışma hem dezeneformasyon hem de mezenformasyonun sektörel olarak yaratacağı riskleri anlamak ve bu risklere karşı alınabilecek tedbirleri sunmayı amaçlamaktadır. Buradan hareketle çalışma dezeneformasyon ve mezenformasyona karşı dijital dönüşüm stratejileri oluşturmayı, siber riskleri belirlemeyi ve değerlendirmeyi, belirli standartlar ve normlar oluşturmayı ve benimsemeyi önermektedir. Bunun yanı sıra mezenformasyon ve dezenformasyonu önlemek için çeşitli endüstriler, sektörler, uluslararası liderler ve liderlere fayda sağlayabilecek ortaklıklarla yatırımları arttırmak önem arz etmektedir.

2. BİLGİ BOZUKLUĞU: MEZENFORMASYON VE DEZENFORMASYON

Öncelikle bilgi bozukluğunu anlamak için, dezenformasyon ve mezenformasyonun ne anlama geldiğini tanımlamak ve netleştirmek gerekmektedir. Mezenformasyon çok geniş kapsamlı olarak yanlış bilgiyi ve bilgi bozukluğunu ifade etmek için kullanılmıştır (Oxford İngilizce Sözlüğü 2020). Mezenformasyon, mevcut durumda, manipülatif veya kötü niyetli olunmadan oluşturulmuş veya paylaşılan yanıltıcı bilgileri tanımlamak için kullanılmaktadır (Ireton ve Posetti, 2018). Dezenformasyon, resmî kurumlar tarafından yabancı bir güce veya medyaya, alıcının politikasını veya görüşünü etkilemek amacıyla sağlananlar da dahil olmak üzere, kasıtlı olarak yanlış bilgilerin yayılması olarak tanımlanmaktadır (Oxford İngilizce Sözlüğü, 2020).

Birleşmiş Milletler, dezenformasyonu, insanlara dürüst olmayan bilgiler sağlayarak insanları şaşırtmaya veya manipüle etmeye yönelik kasıtlı, genellikle düzenlenmiş girişimler olarak tanımlar. Avrupa Komisyonuna göre (2018) dezenformasyon, yanlış veya yanıltıcı olabilecek her türlü bilgi olarak ele alınmaktadır. Yanı sıra komisyon, dezenformasyon sonucu risklerin yalnızca siyasi alanlarda veya kültürel değerlerde yozlaşma gibi gerçekleşmeyeceğini nihayetinde sağlık ve finans sektörlerini de içine alan daha geniş bir alanda zararlı olacağını ifade etmektedir. Dezenformasyonu, ekonomik kazanç sağlamak veya kasıtlı olarak kamuoyunu yanıltmak amacıyla, kamuoyuna zarar verebilecek, doğrulanabilir yanlış veya yanıltıcı bilgilerin

oluşturulması, sunulması ve yayılması olarak tanımlamaktadır (Avrupa Sayıştayı, 2020). Dezenformasyon, ABD Dışişleri Bakanlığı'na göre (Nemr & Gangware, 2019), diğer dezenformasyon tanımlarıyla büyük ölçüde tutarlı olan, yanlış yönlendirme veya zarar verme amaçlı yanlış bilgilerin kasıtlı olarak yayılması olarak geniş çapta tanımlanmaktadır.

Sahte haber, yanlış, uydurma veya kasıtlı olarak yanıltıcı bilgi ileten veya içeren veya bu şekilde nitelendirilen veya okunan haberler olarak tanımlanmaktadır (Oxford İngilizce Sözlüğü, 2020). ABD başkanlık seçimleri terimin popülerlik kazanmasında önemli bir rol sahibidir (NATO, 2020). Sahte haber, iki ana şekilde kullanılmaktadır: Özellikle belirli bir siyasi veya ideolojik amaca hizmet eden, sosyal medyada ve internette dolaşan yanlış haberlere atıfta bulunmak veya taraflı, güvenilmez olarak görülen medya raporlarını itibarsızlaştırmaya çalışmak (Oxford İngilizce Sözlüğü, 2020). Bu tanımlardan bazıları dezenformasyonla örtüşmektedir.

3. SEKTÖREL TEHDİTLER VE İLETİŞİM TEKNOLOJİLERİ

Birçok siber saldırı türü yanıltıcı bilgiler kullanmaktadır. Sosyal mühendislik, sektörlere yönelik en yaygın siber saldırı türüdür (ISACA, 2020). İletişim teknolojilerinin artan kullanımı, sosyal mühendislik tekniklerinde bir artışa yol açmıştır, öyle ki günümüzde çoğu siber saldırı bir tür sosyal mühendislik içermektedir (ENISA, 2020). Sosyal mühendislik teknikleri arasında bahane, yemleme, karşılıksız bırakma, bekleme hattı, sırasını bekleyen ile kimlik avı ve hedefli kimlik avı yer alır (ENISA, 2020). Kimlik avı veya dolandırıcılık amaçlı iletişimler göndermek, giderek yaygınlaşan bir siber tehdittir (Cisco, 2020). Bu nedenle, tanım gereği, kimlik avı yanıltıcı bilgiler kullanır. Kimlik avı, özellikle sektörler için en güçlü tehditlerden biridir ve başlı başına bir sektör haline gelmiştir (Boddy, 2018). Sektörlere yönelik sürekli ve yaygın bir saldırı türüdür, büyük olasılıkla tüm sektörlerde günlük veya saatlik olarak gerçekleşebilmektedir ve sektörlerin yüzde 77'si en az ayda bir kimlik avı saldırısı tecrübe etmiştir (Boddy, 2018, s. 9). 2020'deki banka havalesi üzerinden gerçekleşen siber saldırılar 80 bin 183 dolara mal olmuş ve ülkeler arası ortalama 1,27 milyon dolar zarara sebebiyet verebilecek şekilde sektörleri hedef aldığı bilinmektedir (APWG, 2020).

İletişim teknolojilerinin yaygınlaşması ile pek çok sektör ve kurum iş yapış şeklini değiştirmek zorunda kalmıştır. Giderek kullanımı artan teknolojiler eskiden kas gücü ile yapılan işleri devralmıştır. Bu durum giderek artan bir büyüklükte olan kamu ve özel sektörleri dijitalleştirirken, bu denli büyük bir bilgisayar tabanlı hale gelmenin bir sonucu olarak, sektörler siber risklere karşı daha açık hale gelmiştir. Tüm bilgilerin, gizli evrakların, rekabetle ilgili hassas içeriklerin sızdırılması, çalınması, bozulması mümkün hale gelmiştir. Siber saldırı denildiğinde en yaygın türlerinden biri de sosyal mühendisliktir. Sosyal mühendislik türünde gerçekleşen siber saldırılar %15 iken, gelişmiş kalıcı tehdit (APT- Advanced Persistent Threats) olarak tanımlanan saldırı türleri ise %10 olarak gerçekleşmektedir (ISACA, 2020). Gelişmiş kalıcı tehditler yüksek düzeyde uzmanlık ve önemli kaynaklar gerektirir. Kurumların misyonları, iş fonksiyonları ve bilgi sistemlerini bozmak, zarar vermek amaçlı pek çok aldatma saldırısı veya diğer türlü çoklu saldırı yöntemleri kullanılmaktadır (NIST, 2015).

Gelişmiş kalıcı tehditler dezenformasyon, açık eylemler, gizli siber operasyonlar (yani sosyal mühendislik) ve bir dizi aktör kullanılarak gerçekleşebilmektedir. Siber Tehdit Aktörleri kurumlar üzerinde çeşitli ve kritik etkilere sahip olabilmekte ve önelem alınmazsa kurumları derinden tehdit edebilmektedir. Siber suçlular %22 oranı ile en büyük istismarcılar olmaya devam etmekte ve genellikle kimlik avı yöntemi kullanarak saldırılarını gerçekleştirmektedir (ISACA, 2020). Bir diğer dikkate değer aktör kategorisi de %9 ile ulus/devlet olarak bilinmektedir (ISACA, 2020). Bu yüzde nispeten küçük görünse de ulusal/hükümet siber saldırıları kuruluşlar üzerinde yıkıcı bir etkiye sahip olabilir. Aynı zamanda, sektörlerin büyük çoğunluğunun bu kadar sofistike ve zengin oyunculardan korunamaması da muhtemeldir. Ek olarak, ulus devletler suç grupları, içeriden öğrenenler ve diğer bilgisayar korsanları gibi diğer Siber Tehdit Aktörleri kullanarak siber tehditlerini artırabilir. Siber açıdan yarattığı tehditler açısından düşünüldüğünde ulus devletler ve gelişmiş kalıcı tehditler birbirinin yerine kullanılmıştır (CIS, 2021).

COVID-19 salgını, sektörel tehditleri ve siber güvenlik algısını kökten değiştirdi. Sadece mevcut riskleri artırmakla kalmadı, aynı zamanda yeni tehditler de yarattı. Uzaktan çalışma teknolojilerinin geniş çapta benimsenmesi, müşteriye yönelik ağlarda artan etkinlik ve pandemiye yanıt olarak çevrimiçi hizmetlerin daha yaygın kullanımı siber riskleri artırdı (ICC, 2020). Tüm bu faktörler, sektörler ve müşteriler için saldırı yüzeyini ve siber riskleri artırdı. COVID-19, sektörlerin yanı sıra hükümetlere, kritik altyapılara ve evlere yönelik siber saldırıları körüklemekte ve saldırılar daha karmaşık, hedefli, yaygın ve tespit edilemeyen hale getirmiştir (ENISA, 2020). Bir Interpol (2020) değerlendirmesine göre, COVID-19'un siber suç üzerindeki etkisi, küçük sektörlerden büyük sektörlere, hükümetlere ve kritik altyapıya doğru bir geçiş içinde olduğunu aktarılmaktadır. Aynı zamanda, mikro, küçük ve orta ölçekli sektörler ve çalışanları ile girişimciler ve serbest meslek sahipleri en çok etkilenenler arasında yer almaktadır (ICC, 2020). Mezenformasyon ve dezenformasyonun hızla yayılmasının siber saldırıların

yürütülmesini kolaylaştırmak için kullanılabileceği de gösterilmiştir (Interpol, 2020). Pandemi süresince bir ayda *oltalama* (phishing) dolandırıcılıklarının yüzde 667 arttığı tespit edildi (ENISA, 2020). Genellikle koronavirüs temalı dezenformasyon, siber saldırganlar tarafından yaygın olarak kullanılmaktadır. COVID-19'un ilk günlerinde, koronavirüs temalı spam'de yüzde 6.000 fazla artış oldu (Whitmore, &Parham, 2020). COVID-19 sorunlarının bolluğunda birçok gizli tehdit var. Saldırganlar, marka gibi görünmek için COVID-19 dezenformasyonunu kullanmaktadır böylece bir dizi kötü amaçlı spam, kimlik avı saldırısı ve fidye yazılımıyla çalışanları ve müşterileri kandırmaktadır (Deloitte, 2020). Siber tehditler ve riskler, özellikle pandemi esnasında önemli ölçüde artış göstermiş ve ardından yüksek seviyelerde kalmaya devam etmiştir. Ayrıca, sağlık ve finansal hizmetler gibi sektörlerde büyük güvenlik sorunları ile karşı karşıya kalınmıştır (Panda, 2020).

Medya sektöründe de sürekli olarak bir değişim söz konusudur. Teknoloji ve dijital dönüşüm bu değişimin temel sebeplerindendir (Martens ve diğerleri, 2018). 19. yüzyılın sonlarında medya endüstrisinde çok büyük dönüşümler yaşanmıştır. Bu dönüşüm, Sarı Basın adı verilen yeni bir raporlama ve iş modelinin ortaya çıkmasından sonra meydana gelmiştir. Özellikle tabloid gazeteler, mezenformasyon ve dezenformasyon gibi yeni habercilik biçimlerine bireyleri ve medya kurumlarını teşvik edebilmektedir. Dijital dönüşümün önemli bir özelliği medya sektörünü, doğrusal bir iş modelinden ve çevrimdışı haber yayıncılığından çok yönlü bir pazar/platform iş modeline ve çevrimiçi haber yayıncılığına geçirmek zorunda bırakmasıdır (Martens ve diğerleri, 2018). Ebetteki bu değişim ve dönüşüm medya sektörü için de birtakım riskleri beraberinde getirmiştir.

Sosyal medya, medya endüstrisindeki bir diğer önemli dönüştürücü yenlik olarak görülmektedir. Sosyal medyanın internet tabanlı olduğu ve yeni bir iletişim kanalını meydana getirdiğini pek çok kaynak onaylamaktadır (Carr & Hayes, 2015; Kaplan & Haenlein, 2019). Gazeteler, bağımsız satış noktalarından dev haber pazarlama endüstrilerine geçişi tamamladılar; sonuç olarak, bu kitle iletişim endüstrisi, seri üretim ve kitlesel pazarlamayı doğurmuştur (Daly, 2018). Bu kitlesel pazarlama, reklamcıların işini büyük ölçüde kolaylaştırdı ve nihayetinde gazeteler reklam gelirlerine daha fazla bağımlı hale geldi (Daly, 2018; Griffin, 2019).

Sahte haberler ve sosyal medya hakkında geniş bir literatür bulunmaktadır. Siyasi kutuplaşma ve sosyal medya üzerine yapılan bir literatür taraması, çevrimiçi platformlarda yanlış bilgi ve propagandanın yaygınlığı konusunda geniş bir akademik yayım olduğu sonucuna varmaktadır (Tucker ve diğerleri, 2018, s. 15). Sahte haberlerin belirli web siteleri aracılığıyla yayılmasına ek olarak, literatürün gözden geçirilmesi ve sentezi, ana akım haber medyasının sahte haberlerin daha fazla yayılmasında önemli ve etkin bir rol oynadığını göstermektedir (Tsfati ve diğerleri, 2020). Sahte haberlerle ilişkili birçok olgunun nasıl tanımlanacağı konusunda akademik literatürde çok fazla fikir birliği yoktur (Tucker ve diğerleri, 2018).

Dezenformasyon, sosyal medyanın önemli bir özelliğidir. Birçok siyasi aktör, sosyal medya platformlarında dezenformasyonun yayılmasına ve bunu güçlenmek için kullanmaya dahil olmaktadır (Bradshaw & Howard, 2018). Dünya çapında düzenli internet kullanıcılarının yarısından fazlası, sosyal medya platformlarındaki dezenformasyon tehdidinden endişe duymaktadır (Knuutila ve diğerleri, 2020). Sahte haber siteleri, politikacılar, partizan medya, ana akım medya, hükümetler ve diğer aktörler, sosyal medya ekosisteminde dezenformasyon üretme ve yayma konusunda örtüşen rollere sahiptir (Tucker ve diğerleri, 2018). Dezenformasyonun yayılmasına katkı sağlama konusunda motivasyonlar da farklı olabilir. Siyasi motivasyonları olan devlet destekli aktörler dezenformasyon kampanyalarına katılmaktadır. Öte yandan, küçük Veles kasabasından mali teşviklerle Kuzey Makedon gençleri, reklam tıklamaları için ödeme almak için sahte haberleri yaymak amacıyla ABD'de 140'tan fazla siyasi web sitesi açtı (Kshetri & Voas, 2017). Kuzey Makedon aktörlerin durumu, sosyal medyada finansal motivasyon, değer yaratma ve iş modelleri gibi daha geniş bir konuya ışık tutmaktadır. Etki, sosyal medya pazarlamasında anahtar bir kavram olduğundan, sektörler, önemli bir gelir akışı olan reklamlara erişimlerini ve tıklamalarını artırmanın yollarını aramaktadır (Hanna ve diğerleri, 2011).

Diğer taraftan ABD Hazine Bakanlığı'nın Siber Yaptırımlar Programı 2015'te başladı. Ülke dışından siber destekli faaliyetlerin ABD ulusal güvenliğine, dış politikasına ve ekonomisine yönelik olağandışı ve olağanüstü tehdidini ele almak için ulusal acil durum ilan etti ve 2016'da bu ilanda değişiklikler yaptı. Sektörleri, diğer şeylerin yanı sıra, siber etkin ticari veya rekabet avantajı veya özel mali kazanç yoluyla ABD dışından zimmete para geçirmeye ve ticari sır hırsızlığına karşı koruyan bir çerçevedir (ABD Hazine Bakanlığı, 2017). Bakanlık bu çerçeveyi uyguladı ve 2016 seçimlerini ve diğer çeşitli kötü niyetli faaliyetleri bozmak için siber operasyonlara yaptırımlar uyguladı (ABD Hazine Bakanlığı, 2018). Tipik olarak devletler veya devlet destekli aktörler tarafından gerçekleştirilen, fikri mülkiyet ve sektörlere yönelik siber saldırılar karmaşıktır, APT kimlik avı ve dezenformasyon kullanımını içerir. Siber riskler jeopolitik ve ticaret gibi diğer alanlara da yayılmıştır. Siber iddialar, ABD-Çin ticaret anlaşmazlığını sona erdirmeyi amaçlayan ticaret müzakerelerinin bir parçasıydı (Mitchell & Politi, 2019). Bu durum, bu tür bir siber tehdidin sektörler için önemli bir risk olmaya devam edebileceğini göstermektedir.

4. BİLGİ BOZUKLUĞU İLE SAVAŞ VE SEKTÖREL RİSKLERİ YÖNETME

Mezenformasyon ve dezenformasyon, kamu sektörü ve özel sektör için önemli siber riskler oluşturmaktadır. Dijital çağda dördüncü sanayi devriminin etkilerine tanık olurken, başta sağlık, medya ve finans sektörleri olmak üzere tüm sektörlerde dijital dönüşüm trendinin hâkim olduğu gözlemlenmektedir. Dijital dönüşümle yüzleşmek için sektörler öncelikle hangi teknolojilerin alakalı olduğunu ve iş ortamlarında nasıl uygulanacağını belirlemelidir (Saarikko et al., 2020). Sunucu ve yedekleme alanı olarak kullanılan donanım ve yazılımlardan oluşan eski sistemlerin güvenlik açıkları oluşturduğu ve riski artırdığı yaygın olarak kabul edilmektedir.

İlk olarak, sektör liderleri ve yöneticilerin siber riskin varlığını tanıması gerekir. Siber tehditleri tespit etmek için onları tespit etme yeteneğine sahip olmak çok önemlidir. Sağlık kuruluşlarının siber tehditleri etkili bir şekilde anlama, izleme, raporlama ve yönetme konusundaki sınırlı bir etkinlik alanı bulunmaktadır (Bell ve Ebert, 2015). Pandemi sırasında siber saldırılar daha karmaşık hale geldikçe ve hacimleri önemli ölçüde arttığından bu sorun daha da kötüleşmektedir. Bu tespit sadece sağlıkta değil, diğer alanlarda da bir sorundur. Saldırganlar yöntemlerini geliştirir ve uyarlar; örneğin, kimlik avcıları, tespit edilmekten kaçınmak için güvenliği ihlal edilmiş bir etki alanında bulunabilirler (Jang-Jaccard & Nepal, 2014). Birçok kuruluş bunu fark etmeyebilir ve 2019'daki gibi tüm ihlallerin dörtte birinin aylarca fark edilmemesi gibi olumsuz sonuçlar ortaya çıkabilir (Champion, 2020). Bir diğer önemli eylem, yanıltıcı bilgilerden kaynaklanan siber riskleri ve bunların iş üzerindeki etkilerini anlamaktır. Dezenformasyon ve mezenformasyon gibi bu risklerden bazıları nispeten kolay bir şekilde tanınabilir ve anlaşılabilirken, bazı sorunları değerlendirmek daha zordur. Bu anlamda, bilgi bozukluğunun etkisini yakalayan uygun bir risk değerlendirme çerçevesi esastır.

Dezenformasyon Davranış Kuralları, sektörlerin gönüllü olarak imza attığı küresel bir öz-düzenleyici standartlar organıdır (Avrupa Komisyonu, 2018). Etkili bir standardın iki temel unsuru olmalıdır: Ampirik olarak türetilen teknik veriler ile niteliksel yargılar ve risk toleransı ve strateji gibi yönetsel perspektifler arasındaki boşluğu kapatmak için hem risk değerlendirmesi hem de karar verme modellerini içermelidir (Collier ve diğerleri, 2014).

Dezenformasyonla mücadele için bir dizi araç bulunmaktadır. Bu araçlar, insan doğrulayıcıları olan web sitelerinden botları tespit etmek için yapay zekâ kullanan uygulamalara kadar pek çok biçimde gelir ve birkaç kategoriye ayrılır (RAND, 2019):

(1) bot/spam algılama,

(2) kodlar ve standartlar,

(3) güvenilirlik değerlendirmesi,

(4) dezenformasyon takibi,

(5) eğitim ve öğretim,

(6) doğrulama,

(7) beyaz listeye alma.

Kuruluşlar, dijital dönüşümlerine, genel stratejilerine ve yanıltıcı bilgilerden siber riski yönetme yöntemlerine en uygun olanı seçmelidirler.

Ortaklıkların birçok faydası olabilir. Birincisi, standartların ve ulusal, sektörel veya sektöre özel kılavuzların geliştirilmesini kolaylaştırabilirler. İkincisi, ortaklıklar siber savunmada ölçek ve ölçek ekonomileri yaratır. Üçüncüsü ve en önemlisi, birçok durumda, yüksek düzeyde yaratıcı ve karmaşık devlet destekli saldırıların oluşturduğu siber riskleri azaltmak, kuruluşlar için imkânsız veya son derece maliyetlidir. Bu nedenle, bu siber risklerin ele alınmasında kamu sektörü ile iş birliği, muhtemelen kamu-özel sektör ortaklıkları şeklinde çok önemlidir.

Yukarıdaki önerileri uygulamak için sektörler yeterli fon yatırımı yapmalıdır. Mevcut dezenformasyonla mücadele araçları ve yöntemleri olmasına rağmen, dördüncü sanayi devriminin ilerlemesiyle birlikte yeni teknolojiler gelişmektedir. Bu nedenle araştırma ve geliştirme için daha fazla harcama yapmak kurumlar için önemli hale gelmektedir. Bilgi bozukluğuna ilişkin tedbiren yazılımların edinilmesi, siber savunma harcamaları yapmak da önemli bir konu olarak değerlendirilmelidir. Aynı zamanda her kurumun bir dijital dönüşüm stratejisi olmalı ve bu stratejik planda, siber riskler ve riskler sonrası kayıpları azaltmaya yönelik kriz yönetimi programları gibi işler için gerekli finansal kaynağın ayrılması önemlidir

SONUÇ

Yeni iletişim teknolojilerinin gelişimine paralel olarak gerçekleşen hızlı değişim gündelik hayatı da büyük ölçüde etkilemiştir. Eğitimden, pazarlamaya, iş hayatına, sağlık alanına kadar birçok alanda yeni iletişim teknolojilerinin kullanılmasıyla dezenformasyon ve mezenformasyon artış göstermiştir. Dezenformasyon ve mezenformasyonun artışı bireyler ve toplumlar açısından ciddi tehditler oluştururken kamu sektörü ve özel sektör açısından da gelişmiş kalıcı tehditler oluşturabilmektedir. Bu durum dijital toplum içerisinde varlık sürdürmeye çalışan sektörler açısından oldukça önemli bir sorun olarak karşımıza çıkmaktadır. Bu nedenle bu tehditlere karşı tedbirlerin alınması güvenli teknolojilerin kullanılması bir zorunluluk haline gelmiştir. Aksi halde bilgi bozukluğu olumsuz birçok problem yaratarak iş akışını bozabilmektedir. Özellikle dünyada yaşanan COVID-19 ile birlikte kitle iletişim araçlarından dijital teknolojilerin zorunlu bir şekilde kullanımı bilgi bozukluğunun artmasına neden olmuştur.

Özel sektör, kamu kurum/kuruluşları ve toplumların dijital dönüşümü yeni riskler getirmekte ve sektörler için ortaya çıkan yeni bir tehdit bulunmaktadır. Ortaya çıkan bu tehdit bilgi bozukluğudur. Bilgi bozukluğu genellikle mezenformasyon ve dezenformasyon şeklinde meydana gelmektedir. Bu çalışma, bilgi bozukluğunun, türü fark etmeksizin, sektörel etkisini ve sektörlerin iletişim teknolojilerini kullanması ile birlikte karşılaşacağı muhtemel riskleri anlamaya çalışmıştır. Bu riskler sektörü pek çok açıdan tehdit edebilmektedir. Dolayısıyla konunun daha iyi anlaşılması ve ortaya konması için ileri çalışmalara ve başkaca akademik araştırmalara ihtiyaç olduğu düşünülmektedir. Son olarak, bu çalışma siber riskte bilgi bozukluğu ile başa çıkmak için bazı öneriler sunmaktadır: Dijital dönüşüm stratejileri oluşturmak, siber riskleri belirlemek ve değerlendirmek, standartlar ve normlar belirlemek ve benimsemek, mezenformasyon ve dezenformasyonu önleme ve çeşitli endüstriler, sektörler ve uluslararası liderlerle ve liderlere fayda sağlayabilecek ortaklıklarla yatırımları artırmak.

KAYNAKÇA

ABD Hazine Bakanlığı (2017). Cyber-related sanctions program. Washington, DC: DoT.

ABD Hazine Bakanlığı. (2018). Treasury sanctions Russian cyber actors for interference with the 2016 U.S. elections and malicious cyber-attacks. Available at https:// home.treasury.gov/news/press-releases/sm0312

APWG. (2020, August 27). Phishing activity trends report, 2nd quarter 2020. Anti-Phishing Working Group. Available at https://docs.apwg.org/reports/apwg_trends_report_q2_ 2020.pdf

Avrupa Komisyonu (2018). Final report of the high-level expert group on fake news and online disinformation. Available at https://ec.europa.eu/digital-single-market/ en/news/final-report-high-level-expert-group-fake-newsand-online-disinformation

Avrupa Sayıştayı (2020). EU action plan against disinformation. Available at https://www.eca.europa.eu/ Lists/ECADocuments/AP20_04/AP_Disinformation_EN.pdf

Bell, G., & Ebert, M. (2015). Health care and cyber security: Increasing threats require increased capabilities. KPMG. Available at https://assets.kpmg/content/dam/kpmg/pdf/ 2015/09/cyber-health-care-survey-kpmg-2015.pdf

Boddy, M. (2018). Phishing 2.0: The new evolution in cybercrime. Computer Fraud & Security, 2018(11), 8e10.

Bradshaw, S., & Howard, P. (2018). The global organization of social media disinformation campaigns. Journal of International Affairs, 71(1.5), 23e32.

Carr, C. T., & Hayes, R. A. (2015). Social media: Defining, developing, and divining. Atlantic Journal of Communication, 23(1), 46e65.

Champion, A. (2020, October). Cyber-attack detection challenges and how to meet them. F-secure. Available at https://www.f-secure.com/gb-en/consulting/our-thinking/ challenges-of-cyber-attack-detection

CIS. (2021). Cybersecurity spotlight: Cyber threat actors. Center for Internet Security. Available at https://www. cisecurity.org/spotlight/cybersecurity-spotlight-cyberthreat-actors/

Cisco. (2020). What are the most common cyber-attacks?. Available at https://www.cisco.com/c/en/us/products/ security/common-cyberattacks.html

Collier, Z. A., Dimase, D., Walters, S., Tehranipoor, M. M., Lambert, J. H., & Linkov, I. (2014). Cybersecurity standards: Managing risk and creating resilience. Computer, 47(9), 70e76.

Daly, C. B. (2018). Covering America: A narrative history of a nation's journalism. Amherst, MA: University of Massachusetts Press.

Deloitte. (2020). COVID-19 executive cyber briefing. Available at https://www2.deloitte.com/global/en/pages/risk/covid-19/global-cyber-covid-19-weekly-executive-cyber-briefing.html

ENISA. (2020). ENISA threat landscape. European Union Agency for Cybersecurity. Available at https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

Griffin, B. (2019). Yellow journalism, sensationalism, and circulation wars. New York, NY: Cavendish Square Publishing.

Hanna, R., Rohm, A., & Crittenden, V. L. (2011). We're all connected: The power of the social media ecosystem. Business Horizons, 54(3), 265e273.

ICC. (2020). COVID-19 cyber security threats to MSMEs. International Chamber of Commerce. Available at https://iccwbo.org/content/uploads/sites/3/2020/05/2020-icc-soscybersecurity.pdf

Interpol. (2020). INTERPOL report shows alarming rate of cyberattacks during COVID-19. Lyon, France: International Criminal Police Organization.

Ireton, C., & Posetti, J. (2018). Journalism, 'fake news,' and disinformation. Paris, France: UNESCO.

ISACA. (2020). State of cybersecurity 2020. Schaumburg, IL: Information Systems Audit and Control Association.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), 973e993. J

Kaplan, A., & Haenlein, M. (2019). Digital transformation and disruption: On big data, blockchain, artificial intelligence, and other things. Business Horizons, 62(6), 679e681.

Knuutila, A., Neuder, L., & Howard, P. (2020). Global fears of disinformation. Oxford, UK: Oxford University Press.

Kshetri, N., & Voas, J. (2017). The economics of "fake news." IT Professional, 19(6), 8e12.

Martens, B., Aguiar, L., Gomez-Herrera, E., & Mueller-Langer, F. (2018). The digital transformation of news media and the rise of disinformation and fake news. Digital Economy Working Paper 2018-02, Joint Research Centre Technical Reports. Available at https://dx.doi.org/10.2139/ssrn. 3164170

Mitchell, T., & Politi, J. (2019, April 30). Trump drops cyber theft demands in bid for swift trade deal with China. Financial Times. Available at https://www.ft.com/content/ 3cb5bfda-6b0e-11e9-80c7-60ee53e6681d

NATO. (2020). Media e (Dis)information e security. Available at https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal1-fake-news.pdf

Nemr, C., & Gangware, W. (2019). Weapons of mass distraction: Foreign state-sponsored disinformation in the digital age. Park Advisors. Available at https://www.state.gov/wpcontent/uploads/2019/05/Weapons-of-Mass-DistractionForeign-State-Sponsored-Disinformation-in-the-Digital-Age. pdf

NIST. (2015). Security and privacy controls for federal information systems and organizations. Washington, DC: National Institute for Standards and Technology. OSCE. (2017). Joint declaration on freedom of expression and "fake news," disinformation and propaganda. Vienna, Austria: Organization for Security and Co-Operation in Europe.

Oxford İngilizce Sözlüğü. (2020). Oxford, UK: Oxford University Press.

Panda. (2020). 43 COVID-19 cybersecurity statistics. Available at https://www.pandasecurity.com/en/mediacenter/news/covid-cybersecurity-statistics/ Parham, G., &

Porter, M. E., & Millar, V. E. (1985). How information gives you competitive advantage: The information revolution is transforming the nature of competition. Harvard Business Review, 63(4), 149e160.

RAND. (2019, December 19). Fighting disinformation online: A database of web tools. Available at https://www.rand.org/ research/projects/truth-decay/fighting-disinformation. html

Saarikko, T., Westergren, U. H., & Blomquist, T. (2020). Digital transformation: Five recommendations for the digitally conscious firm. Business Horizons, 63(6), 825e839.

Schwab, K. (2017). *The fourth industrial revolution*. Currency.

Tsfati, Y., Boomgaarden, H. G., Stro¨mba¨ck, J., Vliegenthart, R., Damstra, A., & Lindgren, E. (2020). Causes and consequences of mainstream media dissemination of fake news: Literature review and synthesis. Annals of the International Communication Association, 44(2), 157e173.

Tucker, J., Guess, A., Barbera, P., Vaccari, C., Siegel, A., Sanovich, S., et al. (2018). Social media, political polarization, and political disinformation: A review of the scientific literature. Hewlett Foundation. Available at https://www. hewlett.org/wp-content/uploads/2018/03/Social-MediaPolitical-Polarization-and-Political-DisinformationLiterature-Review.pdf

Whitmore, G. P. W., & Parham, G. (2020). „COVID-19 cyberwar: How to protect your business,". *IBM Institute for Business Value, Iunie*.